Solución de problemas de entornos de LAN Switching

Introducción

Este documento describe las funciones comunes del switch LAN y cómo resolver cualquier problema de conmutación LAN.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Las secciones en este capítulo describen las funciones del LAN Switch y las soluciones a algunos problemas de LAN Switching más comunes. Se tratan los siguientes temas:

- Introducción a LAN Switching
- Sugerencias para solucionar problemas de switch general
- Solucionar problemas de conectividad de puertos
- Resolución de problemas de negociación automática de dúplex medio/completo Ethernet 10/100 Mb
- Trunking ISL en switches de la familia Catalyst 5000 y 6000
- Configuración y solución de problemas de switch EtherChannel a switch
- Utilice Portfast y otros comandos para solucionar los problemas de conectividad de inicio de la estación final
- Configuración y solución de problemas de switching multicapa

Introducción a LAN Switching

Si es nuevo en la conmutación de LAN, estas secciones lo guiarán por algunos de los conceptos principales relacionados con los switches. Uno de los requisitos previos para resolver problemas de cualquier dispositivo es conocer las reglas bajo las cuales funciona. Durante los últimos años, la complejidad de los switches ha aumentado dado que adquirieron mayor popularidad y sofisticación. Estos párrafos describen algunos de los conceptos clave a conocer acerca de los switches.

Ejes de conexión y switches

Debido a la gran demanda que existe en las redes de área local, se ha producido el cambio de una red de ancho de banda compartido, con concentradores y cable coaxial, a una red de ancho de banda dedicada, con switches. Un concentrador permite que varios dispositivos se conecten al mismo segmento de red. Los dispositivos en ese segmento comparten el ancho de banda entre sí. Si se trata de un concentrador de 10 Mb y hay 6 dispositivos conectados a 6 puertos diferentes en el concentrador, los seis dispositivos compartirán los 10 Mb de ancho de banda entre sí. Un concentrador de 100 Mb comparte los 100 Mb de ancho de banda entre los dispositivos conectados. En términos del modelo OSI, un concentrador se considera un dispositivo de capa uno (capa física). Escucha una señal eléctrica en el cable y la transfiere por los otros puertos.

Un switch puede reemplazar físicamente un concentrador en su red. Un switch permite que varios dispositivos se conecten a la misma red, al igual que un concentrador, pero aquí es donde finaliza la similitud. Un switch permite que cada dispositivo conectado tenga ancho de banda dedicado y no ancho de banda compartido. El ancho de banda entre el switch y el dispositivo está reservado para la comunicación hacia y desde ese dispositivo en forma exclusiva. Si hay seis dispositivos conectados a seis puertos diferentes en un switch de 10 Mb, cada uno tiene 10 Mb de ancho de banda con qué trabajar en lugar de compartir ese ancho de banda con los otros dispositivos. Un switch puede incrementar en gran medida el ancho de banda disponible de su red, lo cual puede conducir a una mejora en el rendimiento de la red.

Puentes y switches

Un switch básico se considera un dispositivo de capa dos. Cuando se utiliza la palabra capa, se hace referencia al modelo OSI de 7 capas. Un switch no sólo transmite señales eléctricas, como lo hace un concentrador; en lugar de eso, ensambla las señales en una trama (capa dos) y luego decide qué hacer con la trama. Un switch determina qué hacer con una trama cuando toma prestado un algoritmo de otro dispositivo de red común: un puente transparente. Lógicamente, un switch actúa como lo haría un puente transparente, pero puede administrar tramas mucho más rápidamente que un puente transparente (debido al hardware y arquitectura especiales). Una vez que un switch decide dónde se envía la trama, pasa la trama fuera del puerto (o puertos) apropiado. Puede pensar en un switch como un dispositivo que crea conexiones instantáneas entre varios puertos, trama por trama.

VLAN

Dado que el switch decide, trama por trama, qué puertos intercambian datos, es natural colocar la lógica dentro del switch a fin de permitirle elegir puertos para agrupamientos especiales. A este agrupamiento de puertos se lo denomina Red virtual de área local (VLAN). El switch se asegura que el tráfico de un grupo de puertos nunca se envíe a otros grupos de puertos (los que serán ruteos). Estos grupos de puertos (VLAN) se pueden considerar como un segmento de LAN individual.

Las VLAN también se describen como dominios de difusión. Esto se debe al algoritmo de puente transparente, que decide qué paquetes de difusión (paquetes destinados a la dirección de *todos los dispositivos) se envían por todos los puertos que están en el mismo grupo (es decir, en la misma VLAN).* Todos los puertos que están en la misma VLAN también forman parte del mismo dominio de transmisión.

Algoritmo de puente transparente

El algoritmo de conexión en puente transparente y el árbol de expansión se tratan con más detalle en otro lugar (Capítulo 20: Resolución de problemas de entornos de conexión en puente transparentes). Al recibir una trama, el switch debe decidir qué hará con ella. Podría ignorar la trama; podría pasar la trama fuera de otro puerto, o podría pasar la trama fuera de muchos otros puertos.

Para saber qué hacer con la trama, el switch aprende la ubicación de todos los dispositivos en el segmento. Esta información sobre la ubicación se coloca en la tabla de memoria de contenido direccionable (CAM), denominada así por el tipo de memoria utilizada para almacenar dichas tablas. En la tabla CAM se muestra, para cada dispositivo, la dirección MAC del dispositivo, el puerto en que se puede encontrar esa dirección MAC y con qué VLAN está asociado el puerto. El switch aprende continuamente a medida que se reciben las tramas en el switch. La tabla CAM del switch se actualiza continuamente.

Esta información que se encuentra en la tabla CAM se utiliza para decidir cómo manejar una trama recibida. Para decidir dónde enviar una trama, el switch observa la dirección de destino MAC en la trama recibida y busca esa dirección de destino MAC en la tabla CAM. La tabla CAM muestra a qué puerto se debe enviar la trama para que alcance la dirección MAC de destino especificada. Estas son las reglas básicas que utiliza un switch para llevar a cabo la responsabilidad del reenvío de tramas:

Si se encuentra la dirección MAC de destino en la tabla CAM, entonces el switch enviará la trama por el puerto que esté asociado a esa dirección MAC de destino en la tabla CAM. Está llamada se está desviando.

Si el puerto asociado para enviar la trama es el mismo puerto por el que la trama llegó originalmente, no es necesario enviar la trama hacia el mismo puerto y la trama se ignora. Este proceso se denomina filtrado.

Si la dirección MAC de destino no se encuentra en la tabla CAM (la dirección es *desconocida), el switch emitirá la trama en todos los otros puertos que están en la misma VLAN que la trama recibida.* Esto se denomina inundación. No desborda la trama fuera del puerto en el que se recibió.

Si la dirección MAC de destino de la trama recibida es la dirección de transmisión (FFFF.FFFF.FFFF), la trama se envía a todos los puertos que están en la misma VLAN que la trama recibida. Esto también se denomina saturación. La trama no se envía desde el mismo puerto en el que se recibió.

Spanning Tree Protocol

Como ha visto, el algoritmo de bridging transparente inunda las tramas desconocidas y de

broadcast de todos los puertos que están en la misma VLAN que la trama recibida. Esto causa un posible problema. Si los dispositivos de red que ejecutan este algoritmo se conectan entre sí en un bucle físico, se transmiten tramas saturadas (como difusiones) de switch a switch y alrededor del bucle constantemente. Según las conexiones físicas comprendidas, las tramas pueden multiplicarse exponencialmente debido al algoritmo de saturación, que puede ocasionar graves problemas de red.

Un bucle físico en la red tiene una ventaja: puede proporcionar redundancia. Si un link falla, aún existe otra forma e que el tráfico llegue a su destino. Para permitir los beneficios derivados de la redundancia, y no romper la red debido a la inundación, se creó un protocolo llamado spanning tree. El árbol de expansión fue estandarizado en la especificación IEEE 802.1d.

El propósito del protocolo de árbol de expansión (STP) es identificar y bloquear temporalmente los bucles en un segmento de red o VLAN. Los switches ejecutan el STP y seleccionan un bridge o switch root. Los otros switches miden su distancia desde el switch raíz. Si hay más de una forma para llegar al switch raíz, hay un bucle. Los switches rastrean el algoritmo para determinar qué puertos deben bloquearse para romper el loop. STP es dinámico; si falla un link en el segmento, los puertos que originalmente estaban bloqueando pueden cambiar a modo de reenvío.

Trunking

El enlace troncal es un mecanismo que generalmente se utiliza para permitir que varias VLAN funcionen independientemente a través de varios switches. Los routers y servidores también pueden utilizar enlaces troncales, lo que les permite funcionar simultáneamente en varias VLAN. Si su red sólo tiene una VLAN, no necesita necesariamente conexión troncal; pero si su red tiene más de una VLAN, probablemente desee aprovechar las ventajas de la conexión troncal.

Un puerto en un switch normalmente pertenece a una sola VLAN; cualquier tráfico recibido o enviado en este puerto se supone que pertenece a la VLAN configurada. Por otra parte, un puerto troncal es un puerto que puede ser configurado para enviar y recibir tráfico para varias VLAN. Esto se logra cuando se adjunta la información de la VLAN a cada trama, un proceso denominado *etiquetado de la trama.* Además, el trunking debe estar activo en ambos lados del link; el otro lado debe esperar tramas que incluyan información de VLAN para que se produzca una comunicación adecuada.

Hay métodos diferentes de enlace troncal que dependen de los medios que se utilizan. Los métodos de concentración de link troncal para Fast Ethernet o Gigabit Ethernet son el link entre switches (ISL) o 802.1q. El enlace troncal sobre ATM usa LANE. El enlace troncal por FDDI utiliza 802.10.

EtherChannel

EtherChannel es una técnica que se utiliza cuando se tienen múltiples conexiones al mismo dispositivo. En lugar de que cada enlace funcione de manera independiente, EtherChannel agrupa los puertos para que trabajen como una unidad. Distribuye el tráfico a través de todos los enlaces y brinda redundancia en caso de que uno o más enlaces fallen. Las configuraciones EtherChannel tienen que ser iguales en ambos lados de los links que forman parte del canal. Por lo general, el árbol de expansión bloquea todas estas conexiones paralelas entre los dispositivos porque son bucles, pero EtherChannel se ejecuta *bajo el árbol de expansión, de modo que el árbol de expansión cree que todos los puertos dentro de EtherChannel son un único puerto.*

Conmutación de Capas Múltiple (MLS)

La conmutación multicapa (MLS) es la capacidad de un switch para reenviar tramas en función de la información en el encabezado de capa tres y, a veces, de capa cuatro. Esto generalmente se aplica a los paquetes IP, pero ahora además puede ocurrir con los paquetes IPX. El switch detecta el modo de manejar estos paquetes comunicándose con uno o más routers. Con una breve explicación, el switch observa cómo el router procesa un paquete y, luego, realiza el procesamiento de paquetes futuros en este mismo flujo. Tradicionalmente, los switches eran mucho más rápidos en las tramas de conmutación que los routers, por lo que hacerlos descargar el tráfico proveniente del router puede resultar en importantes mejoras de velocidad. Si algo cambia en la red, el router puede indicarle al switch que borre su memoria caché de capa tres y que la cree desde cero nuevamente a medida que evolucione la situación. El protocolo utilizado para comunicarse con los routers se denomina Protocolo de conmutación de capas múltiples (MLSP).

Cómo obtener más información sobre estas características

Éstas son sólo algunas de las características básicas que admiten los switches. Cada día se agrega más. Es importante comprender cómo funcionan los switches, qué funciones utiliza y cómo deben funcionar dichas funciones. Uno de los mejores lugares para aprender esta información sobre los switches de Cisco es el sitio web de Cisco. Diríjase a la sección *Servicios y soporte y elija Documentos técnicos.* Desde aquí, elija la *página de inicio de la documentación.* Aquí encontrará los conjuntos de documentación para todos los productos de Cisco. El enlace *Multilayer LAN Switches* le lleva a la documentación de todos los switches LAN de Cisco. Para obtener información sobre las características de un switch, lea la *Guía de configuración de software para la versión particular del software que utiliza.* Las guías de configuración de software proporcionan antecedentes sobre lo que la función hace y cuáles son los comandos que deben utilizarse para configurarla en el switch. Toda esta información está disponible en forma gratuita en la Web. Ni siquiera necesita una cuenta para esta documentación; está disponible para cualquier persona. Algunas de estas guías de configuración pueden leerse en una tarde y vale la pena invertir este tiempo.

La otra parte del sitio web de Cisco consta del sitio de soporte y documentación de Cisco. Se completa con información diseñada para ayudarlo a implementar, mantener y solucionar problemas de su red. Diríjase al sitio web Soporte y documentación para obtener información detallada de soporte por tecnologías o productos específicos.

Sugerencia para solucionar problemas del switch general

Existen muchas maneras de solucionar problemas de un switch. A medida que crecen las características de los switches, también aumentan las posibles cosas que puedan irrumpir. Para solucionar los problemas de forma eficaz, desarrolle un enfoque o un plan de pruebas en lugar de un enfoque de aciertos y errores. A continuación, se ofrecen algunas sugerencias generales:

Tómese el tiempo para familiarizarse con el funcionamiento normal del switch. El sitio web de Cisco tiene una gran cantidad de información técnica que describe el funcionamiento de los switches, como se mencionó en la sección anterior. En especial las guías de configuración son muy útiles. Muchos casos se abren y resuelven con información de las guías de configuración de productos.

- Para las situaciones más complejas, tenga un mapa físico y lógico preciso de la red. Un mapa físico muestra la forma en que se conectan los dispositivos y los cables. Un mapa lógico muestra qué segmentos (VLAN) existen en su red y qué routers brindan servicios de routing a

estos segmentos. Un mapa de árbol de expansión es muy útil a la hora de tratar de resolver problemas complejos. Debido a la capacidad de un switch para crear diferentes segmentos con la implementación de VLAN, las conexiones físicas por sí solas no cuentan toda la historia; uno tiene que saber cómo se configuran los switches para determinar qué segmentos (VLAN) existen y saber cómo están conectados lógicamente.

Tenga un plan. Algunos problemas y soluciones son obvios; otros no. Es posible que los síntomas que observa en su red sean el resultado de problemas en otra área o capa. Antes de sacar conclusiones, intente verificar de manera estructurada lo que funciona y lo que no. Dado que las redes pueden ser complejas, es útil aislar los posibles dominios problemáticos. Una manera de llevar esto a cabo es utilizando el modelo OSI de siete capas: Por ejemplo: verifique las conexiones físicas involucradas (capa 1); verifique los problemas de conectividad dentro de la VLAN (capa 2), y verifique los problemas de conectividad entre diferentes VLAN (capa 3), y así sucesivamente. Si hay una configuración correcta en el switch, muchos de los problemas que encuentra están relacionados con problemas de la capa física (puertos físicos y cables). En la actualidad, los switches están involucrados en problemas de capa tres y cuatro, que incorporan inteligencia a los paquetes de switches según la información obtenida de los routers o tienen routers alojados dentro del switch (conmutación de capa tres o cuatro).

No asuma que un componente funciona, debe comprobarlo primero. Esto puede ahorrarle mucho tiempo perdido. Por ejemplo, si una PC no puede iniciar sesión en un servidor a través de la red, hay muchas cosas que pueden ser incorrectas. No se salte las cosas básicas y asuma que algo funciona; alguien puede haber cambiado algo y no le dijo. Solo toma un minuto controlar algunas de las cuestiones básicas (por ejemplo, que los puertos involucrados estén conectados al lugar correcto y estén activos), lo que le ahorrará despilfarrar horas.

Solucionar problemas de conectividad de puertos

¡Si el puerto no funciona, no funciona nada! Los puertos son la base de la red de conmutación. Algunos puertos tienen un significado especial debido a sus ubicaciones en la red y la cantidad de tráfico que llevan. Estos puertos incluyen conexiones con otros switches, routers y servidores. Puede ser más difícil resolver problemas en estos puertos porque, generalmente, aprovechan las funciones especiales como el enlace troncal y EtherChannel. El resto de los puertos también es significativo, ya que conectan a los usuarios reales de la red.

Muchas cosas pueden hacer que un puerto no funcione: problemas de hardware, problemas de configuración y problemas de tráfico. Estas categorías se explorarán con más detalle.

‘Problemas del hardware

General

La funcionalidad de puerto requiere dos puertos activos conectados por un cable activo (del tipo correcto). El valor predeterminado de la mayoría de los switches Cisco es tener un puerto en el estado *notconnect*, lo que significa que actualmente no está conectado a nada, pero quiere conectarse. Si se conecta un buen cable a dos puertos de switch en el *estado no conectado, la luz del enlace debe estar en verde para ambos puertos y el estado del puerto debe ser conectado, lo que significa que el puerto está conectado en lo que concierne a la capa uno.* Estos párrafos señalan los elementos que se deben comprobar si la capa uno no está activa.

Revise el estado del puerto para ambos puertos involucrados. Asegúrense que ningún puerto que forme parte de este link esté cerrado. Es posible que el administrador haya cerrado uno o ambos puertos. El software dentro del switch puede haber apagado el puerto debido a condiciones de error de configuración. Si uno de los lados está apagado y el otro no, el estado del lado habilitado es *not connect* (porque no detecta un vecino del otro lado del cable). El estado en el lado apagado dirá *deshabilitado o error desactivado (según la causa de cierre del puerto).* El enlace no aparecerá, a menos que ambos puertos estén habilitados.

Cuando conecta un buen cable (nuevamente, asumiendo que es del tipo correcto) entre dos puertos activados, estos deben mostrar una luz de enlace verde en pocos segundos. Por otra parte, el estado del puerto aparece como *conectado en la interfaz de la línea de comandos (CLI).* En este punto, si no tiene link, su problema se limita a tres cosas: el puerto en un lado, el puerto en el otro lado, o el cable en el medio. En algunos casos, hay otros dispositivos involucrados: convertidores de medios (de fibra a cobre, etc.), o en enlaces Gigabit puede tener conectores de interfaz gigabit (GBIC). Aún así, esta es un área razonablemente limitada para buscar.

Los conversores de medios pueden agregar ruido a una conexión o debilitar la señal si no funcionan correctamente. También agregan conectores adicionales que pueden causar problemas y son otro componente que debe depurarse.

Verifique conexiones débiles. A veces parece que un cable está instalado en la toma, pero en realidad no lo está; desenchufe el cable y vuelva a insertarlo. También debe buscar suciedad, perdidos o pines rotos. Realice esto para ambos puertos que forman parte de la conexión.

El cable podría estar conectado al puerto incorrecto, lo cual es común. Asegúrese de que ambos extremos del cable estén enchufados a los puertos realmente deseados.

Se puede tener un link en uno de los lados y en el otro no. Verifique la conexión en ambos lados. Un simple cable dañado puede provocar este tipo de problema.

Una luz de link no garantiza que el cable funcione correctamente. Es posible que encuentre una sobrecarga física que haga que funcione en un nivel marginal. Por lo general, esto lo nota el puerto que tiene muchos errores de paquetes.

Para determinar si el problema es el cable, intercámbielo con otro que sepa que es de buena calidad. No lo intercambie con ningún otro cable; asegúrese de que lo intercambia con un cable que sabe que es bueno y del tipo correcto.

Si es una extensión de cable muy larga (por ejemplo, a través de un campus extenso), sería interesante contar con un probador de cables sofisticado. Si no cuenta con un probador de cables, puede considerar lo siguiente:

- Pruebe distintos puertos para ver si se encienden con este cable largo.
- Conecte el puerto en cuestión a otro puerto en el mismo switch solo para ver si el puerto se conecta de manera local.
- Reubique temporalmente los switches a una corta distancia entre sí para probar un cable conocido por su buena calidad.

Cobre

Asegúrese de tener el cable correcto para el tipo de conexión que desea realizar. El cable de categoría 3 puede utilizarse para las conexiones UTP de 10 MB, pero la categoría 5 debe utilizarse para las conexiones 10/100.

Las estaciones finales, los routers o los servidores utilizan un cable de conexión directa RJ-45 para conectarse a un switch o concentrador. Se utiliza un cable cruzado Ethernet para las conexiones de switch a switch o concentrador a switch. Esta es la clavija para un cable cruzado Ethernet. Las distancias máximas para los cables de cobre de Ethernet o Fast Ethernet es de 100 metros. Una buena regla general es que cuando atraviesa una capa OSI, como entre un switch y un router, utilice un cable directo; cuando conecta dos dispositivos en la misma capa OSI, como entre dos routers o dos switches, utilice un cable cruzado. Con el objetivo de aplicar únicamente esta regla, trate a la estación de trabajo como un router.

Estos dos gráficos muestran los pines necesarios para un cable cruzado de switch a switch.

'Fibra'

Para la fibra, asegúrese de que tiene el cable correcto para las distancias involucradas y el tipo de puertos de fibra que se utilizan (monomodo, multimodo). Asegúrese de que los puertos conectados sean puertos de modo único y de modo múltiple. La fibra monomodo generalmente alcanza los 10 kilómetros, y la fibra multimodo generalmente puede llegar a los 2 kilómetros, pero existe el caso especial de 100BaseFX multimodo utilizado en el modo semidúplex, que solo puede llegar a los 400 metros.

Para las conexiones de fibra, asegúrese de que el terminal de transmisión de un puerto esté conectado al terminal de recepción del otro puerto y viceversa; la transmisión para transmitir, la recepción para recibir, no funciona.

Para conexión Gigabit, los GBIC deben coincidir en cada extremo de la conexión. Existen diferentes tipos de GBIC según el cable y las distancias involucradas: longitud de onda corta (SX), longitud de onda larga/largo recorrido (LX/LH) y distancia extendida (ZX).

Un SX GBIC necesita conectarse con un SX GBIC; un SX GBIC no se vincula con un LX GBIC. Además, algunas conexiones Gigabit requieren cables de acondicionamiento según las longitudes implicadas. Consulte las notas de instalación de GBIC.

Si su enlace Gigabit no aparece, compruebe que la configuración de control de flujo y negociación de puerto sea coherente en ambos lados del enlace. Podrían existir incompatibilidades en la implementación de estas funciones si los switches que se conectan son de diferentes proveedores. Si tiene dudas, apague estas funciones en ambos switches.

Problemas de configuración

Otra causa de los problemas de conectividad de puerto es la configuración de software incorrecta del switch. Si un puerto tiene una luz naranja sólida, esto significa que el software dentro del switch apaga el puerto, ya sea por medio de la interfaz de usuario o por procesos internos.

Asegúrese de que el administrador no haya cerrado los puertos involucrados (como se mencionó). El administrador podría cerrar el puerto manualmente en un lado u otro del enlace. Este enlace no aparece hasta que vuelva a activar el puerto; compruebe el estado del puerto.

Algunos switches, como Catalyst 4000/5000/6000, pueden cerrar el puerto en caso de que los procesos de software dentro del switch detecten un error. Cuando vea el estado del puerto, dirá error desactivado. Debe arreglar el problema de configuración y luego sacar manualmente al puerto del estado errDisable. Algunas versiones de software más recientes (CatOS 5.4(1) y

posterior) pueden volver a activar un puerto automáticamente después de un período de tiempo configurable transcurrido en el estado errDisable. Estas son algunas de las causas del estado error desactivado:

Error de configuración de EtherChannel: Si un lado está configurado para EtherChannel y el otro no, puede hacer que el proceso de spanning tree apague el puerto en el lado configurado para EtherChannel. Si intenta configurar EtherChannel pero los puertos involucrados no tienen la misma configuración (velocidad, dúplex, modo troncal, etc.) que sus puertos vecinos a través del link, podría causar el estado errDisable. Es mejor establecer cada lado con el *modo deseado de EtherChannel si desea utilizar EtherChannel.* Más adelante habrá secciones que tratarán la configuración de EtherChannel en detalle.

Discordancia dúplex: Si el puerto del switch recibe muchas colisiones tardías, esto generalmente indica un problema de discordancia dúplex. Existen otras causas para las colisiones tardías: una NIC defectuosa, segmentos de cable que son demasiado largos, pero la razón más común hoy en día es una discordancia dúplex. El lado de dúplex completo considera que puede enviar siempre que lo desee. El lado semidúplex solo espera paquetes en determinados momentos, no en "ningún" momento.

Protección de puertos BPDU: Algunas versiones más recientes del software del switch pueden monitorear si portfast está habilitado en un puerto. Un puerto que utiliza PortFast debe estar conectado a una estación final, no a dispositivos que generan paquetes de árbol de expansión llamados BPDU. Si el switch nota que una BPDU que viene en un puerto tiene habilitado PortFast, pondrá el puerto en modo de error desactivado.

UDLD: Unidirectional Link Detection es un protocolo en algunas versiones nuevas de software que detecta si la comunicación a través de un link es unidireccional solamente. Un cable de fibra roto u otros problemas de cable/puerto pueden causar esta comunicación unidireccional solamente. Estos links parcialmente funcionales pueden producir problemas cuando los switches involucrados no conocen que el link está dañado parcialmente. Con este problema, pueden producirse loops de árbol de expansión. La UDLD puede configurarse para poner un puerto en estado de error desactivado si detecta un enlace unidireccional.

Discordancia de VLAN nativa: antes de que un puerto tenga activada la conexión troncal, pertenece a una sola VLAN. Cuando se activa la conexión troncal, el puerto puede transmitir el tráfico para varias VLAN. El puerto todavía recuerda la VLAN en la que se encontraba antes de que se activara el enlace troncal; que se denomina VLAN nativa. La VLAN nativa es fundamental para la conexión troncal 802.1q. Si la VLAN nativa ubicada en cada extremo del enlace no coincide, el puerto entra en rl estado de error desactivado.

Otro: Cualquier proceso dentro del switch que reconozca un problema con el puerto puede colocarlo en el estado *errDisable*.

Otra causa de los puertos inactivos es la desaparición de la VLAN a la que pertenecen. Cada puerto de un switch pertenece a una VLAN. Si se elimina la VLAN, el puerto queda inactivo. Algunos switches muestran una luz naranja constante en cada puerto en que esto ha sucedido. Si llega a trabajar un día y ve cientos de luces naranja, no entre en pánico; podría ser que todos los puertos pertenecían a la misma VLAN y alguien eliminó accidentalmente la VLAN a la que

pertenecían los puertos. Cuando vuelva a agregar la VLAN a la tabla de VLAN, los puertos volverán a estar activos. Un puerto recuerda su VLAN asignada:

Si usted tiene link y los puertos aparecen conectados, pero no puede establecer comunicación con otro dispositivo, esto puede resultar particularmente desconcertante. Por lo general, indica un problema superior a la capa física: capa 2 o capa 3. Prueba estas cosas.

Verifique el modo de trunking en cada lado del link. Asegúrese de que ambos lados estén en el mismo modo. Si activa el modo de enlace troncal en "on" (en lugar de en "auto" o "desirable") para un puerto y el otro puerto tiene el enlace troncal

modo establecido en "off", no se pueden comunicar. La conexión troncal cambia el formato del paquete; los puertos deben aceptar el formato que utilizan en el enlace o no se entienden entre sí.

Asegúrese de que todos los dispositivos se encuentren en la misma VLAN. Si no están en la misma VLAN, entonces se debe configurar un router para permitir que los dispositivos se comuniquen.

Asegúrese de que el direccionamiento de la capa tres esté correctamente configurado.

Problemas de tráfico

En esta sección se describen algunas de las cosas que puede aprender cuando observa la información de tráfico de un puerto. La mayoría de los switches tienen alguna manera de rastrear los paquetes cuando entran y salen de un puerto. Los comandos que generan este tipo de salida en los switches Catalyst 4000/5000/6000 **son show portandshow mac**. El resultado de estos comandos en los switches 4000/5000/6000 se describe en las referencias de los comandos del switch.

Algunos de estos campos de tráfico de puerto muestran cuánta información se transmite y se recibe en el puerto. Otros campos muestran la cantidad de tramas con errores que se encuentran en el puerto. Una gran cantidad de errores de alineación, errores de FCS o colisiones tardías puede indicar una incompatibilidad de dúplex en el cable. Otras causas de estos tipos de problemas pueden ser tarjetas de interfaz de red defectuosas o problemas de cable. Si tiene una gran cantidad de tramas diferidas, es una señal de que su segmento tiene demasiado tráfico; el switch no puede enviar suficiente tráfico en el cable para vaciar sus búferes. Analice la posibilidad de trasladar ciertos dispositivos a otro segmento.

Falla de hardware del switch

Si ha intentado todo lo que se le ocurrió y el puerto no funciona, puede haber hardware defectuoso.

A veces, los puertos se dañan mediante una descarga electroestática (ESD). Es posible que vea o no una indicación de esto.

Vea los resultados de power-on self-test (POST) en el switch para ver si se ha indicado alguna falla para alguna parte del switch.

Si observa un comportamiento que solo se puede considerar "extraño", esto podría indicar problemas de hardware, pero también problemas de software. Normalmente, es más sencillo volver a cargar el software que obtener un nuevo hardware. Primero intente trabajar con el software del switch.

El sistema operativo puede tener un error. Si carga un sistema operativo más nuevo, podría solucionarlo. Puede investigar los errores conocidos leyendo las notas de la versión del código que utiliza o mediante Bug ToolKit de Cisco.

El sistema operativo podría estar dañado de algún modo. Si vuelve a cargar la misma versión del sistema operativo, podría solucionar el problema.

Si la luz de estado del switch parpadea y es de color naranja, generalmente indica que hay algún tipo de problema de hardware con el puerto, el módulo o el switch. Lo mismo sucede si el estado de puerto o módulo es defectuoso.

Antes de cambiar el hardware del switch, puede intentar algunas cosas:

Vuelva a colocar el módulo en el switch. Si hace esto con la energía encendida, asegúrese de que el módulo admita el reemplazo en caliente. En caso de duda, apague el switch antes de volver a colocar el módulo o consulte la guía de instalación de hardware. Si el puerto está integrado en el switch, ignore este paso.

Reinicie el switch A veces, esto hace que el problema desaparezca; se trata de una solución alternativa, no de una solución.

Revise el software del switch. Si es una nueva instalación, recuerde que algunos componentes solo pueden trabajar con determinadas versiones de software. Revise las notas de la versión o la guía de instalación y configuración de hardware del componente que instala.

Si está razonablemente seguro de que tiene un problema de hardware, reemplace el componente defectuoso.

Resolución de problemas de negociación automática de dúplex medio/completo de Ethernet 10/100 Mb

Objetivos

Esta sección presenta información general utilizada para resolver problemas y una discusión de técnicas para resolver problemas de negociación automática de Ethernet.

Esta sección muestra cómo determinar el comportamiento actual de un link. Continúa mostrando cómo los usuarios pueden controlar la conducta y explicar las situaciones cuando la negociación automática falla.

Muchos Switches Catalyst de Cisco y Routers de Cisco soportan la autonegociación. Esta sección se centra en la negociación automática entre switches Catalyst 5000. Los conceptos

que se explican aquí también pueden aplicarse a los demás tipos de dispositivos.

Introducción

La negociación automática es una función opcional de la norma Fast Ethernet de IEEE 802.3u que permite a los dispositivos intercambiar información automáticamente por un link sobre capacidades dúplex y de velocidad.

La negociación automática está destinada a los puertos, los cuales están asignados a los áreas donde los dispositivos o usuarios transitorios se conectan a una red. Por ejemplo, muchas compañías les dan oficinas compartidas o cubículos a sus ejecutivos de cuentas e ingenieros en sistemas para que usen cuando están en la oficina en lugar de en la calle. Cada oficina o cubículo tiene un puerto Ethernet conectado de forma permanente a la red de la oficina. Debido a que es posible que no se pueda garantizar que cada usuario tenga Ethernet de 10 Mb o 100 Mb o una tarjeta de 10/100 Mb en su computadora portátil, los puertos del switch que manejan estas conexiones deben ser capaces de negociar el modo de velocidad y dúplex. La alternativa consiste en suministrar tanto un puerto de 10 Mb como uno de 100 Mb en cada oficina o cubículo y etiquetarlos en consecuencia.

No se debe utilizar la negociación automática para los puertos que admiten dispositivos de infraestructura de redes, como switches y routers, u otros sistemas de extremos estáticos, como servidores e impresoras. A pesar de que el modo de negociación automática de velocidad y dúplex es, por lo general, el comportamiento predeterminado en los puertos del switch con capacidad para hacerlo, los puertos que están conectados a dispositivos fijos siempre deben configurarse según el comportamiento correcto y no se les debe permitir negociarlo. Esto elimina cualquier posible problema de negociación y garantiza que siempre sepa exactamente cómo deben funcionar los puertos. Por ejemplo, un enlace Ethernet de switch a switch de 10/100BaseTX configurado para un dúplex competo de 100 Mb solo funciona en ese modo y esa velocidad. No hay posibilidad de que los puertos reduzcan el enlace a una menor velocidad durante la restauración de un puerto o la restauración de un switch. En el caso de que los puertos no puedan operar como han sido configurados, no deben pasar tráfico. Por otro lado, un link de switch a switch al que se le ha permitido negociar su comportamiento puede funcionar en semidúplex de 10 Mb. Normalmente, resulta más fácil detectar un enlace no operativo que un enlace operativo que no está funcionando a la velocidad esperada o en el modo esperado.

Una de las causas más comunes de problemas de rendimiento en los links Ethernet de 10/100Mb es cuando un puerto en el link funciona en semidúplex, mientras que el otro puerto funciona en dúplex completo. Esto ocurre en ocasiones cuando se restaura uno o ambos puertos de un enlace y el proceso de negociación automática no logra que ambos socios de enlace tengan la misma configuración. También sucede cuando los usuarios vuelven a configurar sólo un lado de un link y se olvidan de volver a configurar el otro lado. Muchas llamadas de soporte relacionadas con el rendimiento se pueden evitar creando una política que requiera que los puertos para todos los dispositivos no transitorios se configuren para su comportamiento requerido y reforzando la política con medidas de control de cambio adecuadas.

Resolución de problemas de negociación automática de Ethernet entre dispositivos de infraestructura de red

Procedimientos y/o escenarios

Escenario 1. Cat 5K con Fast Ethernet

Tabla 22-2: Problemas de Conectividad de Negociación Automática

Posible problema	Solución
¿El comportamiento actual del enlace se negoció automáticamente?	1. Utilice **el comando show port mod_num/port**_number para determinar el comportamiento actual del link. Si ambos socios de enlace (interfaces en cualquier extremo del enlace) indican que tienen un prefijo "a-" en sus campos de estado de dúplex y velocidad, la negociación automática probablemente se realizó de forma correcta.
negociación automática no admitida.	2. Ejecute **el comando show port capabilities mod_num/port**_number para verificar que sus módulos soporten la negociación automática.
la negociación automática no funciona en los switches Catalyst.	3. Utilice el comando **set port speed mod_num/port_num** autocommand en un Catalyst para configurar la negociación automática. 4. Pruebe con diferentes puertos o módulos. 5. Intente restablecer los puertos. 6. Pruebe con cables de interconexiones diferentes. 7. Apague los dispositivos y vuelva a encenderlos.
la negociación automática no funciona en los routers de Cisco.	8. Ejecute el comando correcto del IOS de Cisco para habilitar la negociación automática (si está disponible) 9. Pruebe con interfaces diferentes. 10. Intente restablecer las interfaces. 11. Pruebe con cables de interconexiones diferentes. 12. Apague los dispositivos y vuelva a encenderlos.

Ejemplo de Negociación Automática de Configuración y Troubleshooting de Ethernet 10/100Mb

Esta sección examina el comportamiento de un puerto Ethernet 10/100Mb que soporta la negociación automática. También le mostrará cómo realizar cambios en el comportamiento predeterminado y cómo restaurar el comportamiento predeterminado.

Tareas que realizar

Examine las capacidades de los puertos.

Configure la negociación automática para el puerto 1/1 en ambos switches.

Determine si el modo velocidad y dúplex están configurados en negociación automática.

Cambie la velocidad en el puerto 1/1 del switch A a 10 Mb.

Comprenda el significado del prefijo "a-" en el dúplex y los campos de estado de velocidad.

Vea el estado dúplex del puerto 1/1 en el switch B.

Interprete el error de discordancia dúplex.

Interprete los mensajes de error del spanning tree.

Cambie el modo dúplex a semidúplex en el puerto 1/1 del Switch A.

Configure el modo dúplex y la velocidad del puerto 1/1 en el switch B.

Restaure el modo de dúplex y la velocidad predeterminados en los puertos 1/1 en ambos switches.

Vea los cambios del estado del puerto en ambos switches.

Paso a paso

Siga estos pasos:

El comando **show port capabilities 1/1** muestra las capacidades de un puerto Ethernet 10/100BaseTX 1/1 en el Switch A.

Ingrese este comando para los dos puertos en los que está resolviendo problemas. Ambos puertos deben soportar las capacidades de velocidad y dúplex mostradas si se supone que deben utilizar la negociación automática.

```
Switch-A> (enable) show port capabilities 1/1
Model WS-X5530
Port 1/1
Type 10/100BaseTX
Speed auto,10,100
Duplex half, full
```

La negociación automática se configura para el modo de velocidad y dúplex en el puerto 1/1 de ambos switches si ingresa el comando **set port speed 1/1 auto** (auto es el valor predeterminado para los puertos que soportan la negociación automática).

```
Switch-A> (enable) set port speed 1/1 auto
Port(s) 1/1 speed set to auto detect.
Switch-A (enable)
```

Nota: El comando **set port speed {mod_num/port_num} auto** también establece el modo dúplex en auto. No existe ningún comando set port duplex {mod_num/port_num} auto.

El comando show port 1/1muestra el estado de los puertos 1/1 en los switches A y B.

```
Switch-A> (enable) show port 1/1
```

```
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- -----
 1/1               connected  1          normal a-full a-100 10/100BaseTX

Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- -----
 1/1               connected  1          normal a-full a-100 10/100BaseTX
```

Observe que la mayor parte del resultado normal del comando show port {mod_num/port_num} ha sido omitido.

Los prefijos "a-" en "full" y "100" indican que este puerto no se ha definido (configurado) para una velocidad o modo dúplex específico. Por lo tanto, puede negociar automáticamente su modo dúplex y velocidad si el dispositivo al que está conectado (su socio de link) también puede negociar automáticamente su modo dúplex y velocidad. También observe que el estado es "connected" (conectado) en ambos puertos, lo que significa que el otro puerto ha detectado un pulso de link. El estado puede ser “conectado” aún si el dúplex ha sido negociado incorrectamente o mal configurado.

Para demostrar qué sucede cuando un socio de link negocia automáticamente y el otro socio de link no negocia, la velocidad en el puerto 1/1 en el Switch A se establece en 10Mb con el comando **set port speed 1/1 10**.

```
Switch-A> (enable) set port speed 1/1 10
Port(s) 1/1 speed set to 10Mbps.
Switch-A> (enable)
```

Nota: Si codifica la velocidad en un puerto, inhabilita toda la funcionalidad de negociación automática en el puerto para velocidad y dúplex.

Cuando se ha configurado un puerto para una velocidad, su modo dúplex se configura automáticamente para el modo negociado anteriormente. En este caso, dúplex completo. Cuando ingresa el comando set port speed 1/1 10, hace que el modo dúplex en el puerto 1/1 se configure como si también hubiese ingresado el comando set port duplex 1/1 full . Esto se explica a continuación.

Comprenda el significado del prefijo "a-" en los campos de estado de velocidad y dúplex.

La ausencia del prefijo "a-" en los campos de estado del resultado del comando show port 1/1 en el switch A indica que el modo dúplex está ahora configurado como "completo" y que la velocidad está configurada en "10."

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal  full  10    10/100BaseTX
```

El comando **show port 1/1** en el Switch B indica que el puerto ahora funciona en semidúplex y 10Mb.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-half a-10  10/100BaseTX
```

Este paso muestra que es posible que un partner de link detecte la velocidad a la que opera el otro partner de link a pesar de que el otro partner de link no esté configurado para la negociación automática. Detectando el tipo de señal eléctrica que llega para descubrir si es 10Mb o 100Mb hace esto. Así es como el Switch B determinó que el puerto 1/1 debe funcionar a 10Mb.

No es posible detectar el modo dúplex correcto de la misma forma que se puede detectar la velocidad correcta. En este caso, cuando el puerto 1/1 del switch B se configura para la negociación automática y el puerto del switch A no, se obliga al puerto 1/1 del switch B a seleccionar el modo de dúplex predeterminado. En los puertos Ethernet de Catalyst, el modo predeterminado es negociación automática y, si falla la negociación automática, semidúplex.

Este ejemplo también muestra que un link puede ser conectado exitosamente cuando no coinciden los modos de dúplex. El puerto 1/1 en el Switch A está configurado para dúplex completo mientras que el puerto 1/1 en el Switch B tiene de forma predeterminada el semidúplex. Para evitar esto, siempre configure ambos socios de enlace.

El prefijo "a-" en los campos de estado Duplex (Dúplex) y Speed (Velocidad) no siempre significa que se ha negociado el comportamiento actual. A veces sólo significa que el puerto no ha sido configurado para velocidad o modo dúplex. El resultado anterior del Switch B muestra el Dúplex como "a-half" y la Velocidad como "a-10", lo que indica que el puerto funciona a 10 Mb en el modo semidúplex. En este ejemplo, el socio de link en este puerto (puerto 1/1 en el Switch A) está configurado para "full" y "10Mb". No fue posible que el puerto 1/1 en el Switch B haya negociado automáticamente su comportamiento actual. Esto prueba que el prefijo "a-" sólo indica la voluntad de realizar la negociación automática, pero no que la negociación automática se haya realizado realmente.

Comprenda el mensaje de error de la incompatibilidad de dúplex.

Este mensaje acerca de la incompatibilidad del modo dúplex se refleja en el switch A después de que la velocidad en el puerto 1/1 cambia a 10 Mb. La discordancia fue causada por el puerto 1/1 del Switch B, que de forma predeterminada es semidúplex porque detectó que su socio de link ya no podía realizar la negociación automática.

```
%CDP-4-DUPLEXMISMATCH:Full/half-duplex mismatch detected o1
```

Es importante tener en cuenta que a este mensaje lo crea el Protocolo de detección de Cisco (CDP), y no el protocolo de negociación automática 802.3. El CDP puede informar sobre problemas que detecta, pero generalmente no los corrige de manera automática. Una incompatibilidad de dúplex puede o no generar un mensaje de error. Otra indicación de una discordancia dúplex son los errores de alineación y FCS rápidamente aumentados en el lado semidúplex y los "fragmentos minúsculos" en el puerto dúplex completo (como se ve en un

puerto sh {mod_num/port_num}).

Comprenda los mensajes del árbol de expansión.

Además del mensaje de error de incompatibilidad de dúplex del paso 8, es posible que también observe los siguientes mensajes del árbol de expansión cuando cambie la velocidad en un enlace. Una discusión sobre el Spanning Tree está más allá del alcance de este documento; consulte el capítulo sobre Spanning Tree para obtener más información sobre Spanning Tree.

```
%PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1
```

Para demostrar lo que sucede cuando el modo dúplex ha sido configurado, el modo en el puerto 1/1 en el switch A se establece en semidúplex mediante el comando set port duplex 1/1 half.

```
Switch-A> (enable) set port duplex 1/1 half
Port(s) 1/1 set to half-duplex.
Switch-A> (enable)
```

El comando show port 1/1 muestra el cambio en el modo Duplex en este puerto.

```
Switch-A> (enable) sh port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal half   10    10/100BaseTX
```

En este momento, los puertos 1/1 en ambos switches funcionan en semidúplex. Sin embargo, el puerto 1/1 del switch B todavía está configurado para negociar automáticamente, como se muestra en el siguiente resultado del comando show port 1/1.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-half a-10  10/100BaseTX
```

Este paso muestra cómo configurar el modo dúplex en el puerto 1/1 del switch B en semidúplex. Esto es consistente con la política recomendada para configurar los dos socios de enlace de la misma forma.

Para implementar la política de modo que se configuren ambos socios de enlace para el mismo comportamiento, este paso establece ahora el modo dúplex a la mitad y la velocidad en 10 en el puerto 1/1 en el switch B.

Este es el resultado cuando ingresa el comando **set port duplex 1/1 half** en el Switch B:

```
Switch-B> (enable) set port duplex 1/1 half
Port 1/1 is in auto-sensing mode.
Switch-B> (enable)
```

El comando set port duplex 1/1 half falló porque no es válido si la negociación automática está habilitada. Esto también significa que este comando no inhabilita la negociación automática. La negociación automática solo se puede deshabilitar con set port speed {mod_num/port_num {10. **| 100} }** .

Este es el resultado cuando ingresa el comando **set port speed 1/1 10** en el Switch B:

```
Switch-B> (enable) set port speed 1/1 10
Port(s) 1/1 speed set to 10Mbps.
Switch-B> (enable)
```

Ahora, el comando set port duplex 1/1 half en el switch B funciona:

```
Switch-A> (enable) set port duplex 1/1 half
Port(s) 1/1 set to half-duplex.
Switch-A> (enable)
```

El comando **show port 1/1** en el Switch B muestra que los puertos ahora están configurados para semidúplex y 10Mb.

```
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal half   10    10/100BaseTX
```

> **Nota**: El **puerto set duplex {mod_num/port_num {half | full }}** depende del **comando set port speed {mod_num/port_num {10 | 100 }}** . En otras palabras, debe configurar la velocidad antes de activar el modo dúplex.

Configure los puertos 1/1 en ambos switches para que negocien automáticamente con el comando **set port speed 1/1 aut**.

```
Switch-A> (enable) set port speed 1/1 auto
Port(s) 1/1 speed set to auto detect.
Switch-A> (enable)
```

> **Nota**: Una vez que un modo dúplex de un puerto se ha configurado en un modo distinto de automático, la única manera de configurar el puerto para que detecte automáticamente su modo dúplex es ejecutar el comando **set port speed**

{mod_num/port_num} auto. No existe ningún comando set port duplex {mod_num/port_num} auto. En otras palabras, si ejecuta el comando **set port speed {mod_num/port_num} auto**, restablece la detección de velocidad de puerto y la detección de modo dúplex en auto.

Examine el estado de los puertos 1/1 en ambos switches mediante el comando show port 1/1.

```
Switch-A> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-full a-100 10/100BaseTX
Switch-B> (enable) show port 1/1
Port  Name         Status     Vlan       Level  Duplex Speed Type
----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1               connected  1          normal a-full a-100 10/100BaseTX
```

Ahora, ambos puertos están configurados con su comportamiento predeterminado de negociación automática. Ambos puertos han negociado dúplex completo y 100 Mb.

Antes de llamar al equipo de soporte técnico de Cisco Systems

Antes de llamar al sitio web de soporte técnico de Cisco Systems, asegúrese de leer este artículo y de completar las acciones sugeridas para los problemas del sistema. Además, documente los resultados para que Cisco pueda ayudarlo a:

Capture el resultado de **show** version de todos los dispositivos afectados.

Capture el resultado del comando show port mod_num/port_num de todos los puertos afectados.

Capture el resultado de show port mod_num/port_num capabilities desde todos los puertos afectados.

Configuración de las conexiones de switch a switch EtherChannel en los switches Catalyst 4000/5000/6000

EtherChannel permite la combinación de múltiples links físicos Fast Ethernet o Gigabit Ethernet en un canal lógico. Esto permite que el tráfico entre los links comparta la carga en el canal, así como la redundancia en caso de que uno o más links en el canal fallen. EtherChannel se puede utilizar para interconectar switches, routers, servidores y clientes de LAN a través de un cableado de par trenzado no apantallado (UTP) o de fibra monomodo y multimodo.

EtherChannel es una manera fácil de agregar ancho de banda entre dispositivos de red críticos. En Catalyst 5000 puede crearse un canal a partir de dos puertos convirtiéndolo en un enlace de

200 Mbps (dúplex completo de 400 Mbps) o de cuatro puertos convirtiéndolo en un enlace de 400 Mbps (dúplex completo de 800 Mbps). Algunas tarjetas y plataformas también admiten Gigabit EtherChannel y tienen la capacidad de utilizar entre dos y ocho puertos en un EtherChannel. El concepto es el mismo sin importar las velocidades o la cantidad de links involucrados. Normalmente, el protocolo de árbol de extensión (STP) considera que estos enlaces redundantes entre dos dispositivos son bucles y establece los enlaces redundantes en modo de bloqueo. Esto hace que estos links sean inactivos (que proporcionan solamente capacidades de respaldo si el link principal falla). Cuando utiliza Cisco IOS 3.1.1 o superior, el spanning tree trata el canal como un gran link, de modo que todos los puertos en el canal pueden estar activos al mismo tiempo.

Esta sección lo guiará a través de los pasos para configurar EtherChannel entre dos switches Catalyst 5000 y ver los resultados de los comandos mientras se ejecutan. Los switches Catalyst 4000 y 6000 podrían haberse utilizado en las situaciones presentadas en este documento para obtener los mismos resultados. Para Catalyst 2900XL y 1900/2820, la sintaxis del comando es diferente, pero los conceptos de EtherChannel son los mismos.

EtherChannel se puede configurar manualmente si ingresa los comandos apropiados o se puede configurar automáticamente si el switch negocia el canal con el otro lado utilizando el protocolo de agregación de puertos (PAgP). Se recomienda utilizar el modo deseado del PAgP para configurar EtherChannel siempre que sea posible, ya que la configuración manual de EtherChannel puede crear algunas complicaciones. Este documento brindará ejemplos de cómo configurar EtherChannel manualmente y ejemplos de cómo configurar EtherChannel mediante el PAgP. También se incluye cómo resolver problemas de EtherChannel y cómo usar el enlace troncal con EtherChannel. En este documento, los términos EtherChannel, Fast EtherChannel, Gigabit EtherChannel o canal hacen referencia a EtherChannel.

Contenido

Esta figura ilustra este entorno de prueba. La configuración de los switches se ha borrado con el comando clear config all. Por lo tanto, el mensaje de solicitud se cambió utilizando set system name. Se asignaron una dirección IP y una máscara al switch para fines de administración con **set int sc0 172.16.84.6 255.255.255.0** para el SwitchA y **set int sc0 172.16.84.17 255.255.255.0</ /strong>para el SwitchB. Se asignó un gateway predeterminado a ambos switches con set ip route default 172.16.84.1.**

Las configuraciones del switch se borraron para que comenzaran a partir de las condiciones predeterminadas. A los switches se les dio nombres para identificarlos desde el símbolo del

sistema en la línea de comandos. Las direcciones IP se asignaron para que pudiera hacer ping entre los switches y probarlas. No se usó la gateway predeterminada.

Muchos de los comandos muestran más resultados de los necesarios. El resultado externo se elimina de este documento.

Tareas para la configuración manual de EtherChannel

Este es un resumen de las direcciones para configurar manualmente EtherChannel:

Mostrar la versión de Cisco IOS y los módulos utilizados en este documento.

Verifique la compatibilidad de EtherChannel con los puertos.

Verifique que los puertos se encuentren conectados y en funcionamiento.

Verifique que los puertos a agrupar tengan la misma configuración.

Identifique grupos de puertos válidos.

Cree el canal

Paso a paso

Estos son los pasos para configurar manualmente EtherChannel.

El comando show version muestra la versión de software que ejecuta el switch. **El comando show** module enumera los módulos que se instalan en el switch.

```
Switch-A show version
WS-C5505 Software, Version McpSW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
?

Switch-A show module
Mod Module-Name         Ports Module-Type           Model    Serial-Num Status
--- ------------------- ----- --------------------- --------- --------- -------
1                       0     Supervisor III        WS-X5530  006841805 ok
2                       24    10/100BaseTX Ethernet WS-X5225R 012785227 ok
?
```

Verifique que EtherChannel esté soportado en los puertos y que **show port** capabilities aparezca en las versiones 4.x y posteriores. Si tiene un IOS de Cisco anterior a 4.x, debe

omitir este paso. No todos los módulos Fast Ethernet admiten EtherChannel. Algunos de los módulos EtherChannel tienen "Fast EtherChannel" escrito en la esquina inferior izquierda del módulo (como se ve en el switch) lo que significa que la función es admitida. Esta convención fue abandonada en los módulos posteriores. Los módulos en esta prueba no tienen “Fast EtherChannel” impreso en ellos, pero son compatibles con la función.

```
Switch-A show port capabilities
Model                   WS-X5225R
Port                    2/1
Type                    10/100BaseTX
Speed                   auto,10,100
Duplex                  half,full
Trunk encap type        802.1Q,ISL
Trunk mode              on,off,desirable,auto,nonegotiate
Channel                 2/1-2,2/1-4
Broadcast suppression   percentage(0-100)
Flow control            receive-(off,on),send-(off,on)
Security                yes
Membership              static,dynamic
Fast start              yes
Rewrite                 yes
Switch-B show port capabilities
Model                   WS-X5234
Port                    2/1
Type                    10/100BaseTX
Speed                   auto,10,100
Duplex                  half,full
Trunk encap type        802.1Q,ISL
Trunk mode              on,off,desirable,auto,nonegotiate
Channel                 2/1-2,2/1-4
Broadcast suppression   percentage(0-100)
Flow control            receive-(off,on),send-(off,on)
Security                yes
Membership              static,dynamic
Fast start              yes
Rewrite                 no
```

Un puerto que no admite EtherChannel es similar a esto:

```
Switch show port capabilities
Model                   WS-X5213A
Port                    2/1
Type                    10/100BaseTX
Speed                   10,100,auto
Duplex                  half,full
Trunk encap type        ISL
Trunk mode              on,off,desirable,auto,nonegotiate
```

```
Channel                 no
Broadcast suppression   pps(0-150000)
Flow control            no
Security                yes
Membership              static,dynamic
Fast start              yes
```

Verifique que los puertos se encuentren conectados y en funcionamiento. Antes de conectar los cables, este es el estado del puerto.

```
Switch-A show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     notconnect 1          normal   auto  auto 10/100BaseTX
 2/2                     notconnect 1          normal   auto  auto 10/100BaseTX
 2/3                     notconnect 1          normal   auto  auto 10/100BaseTX
 2/4                     notconnect 1          normal   auto  auto 10/100BaseTX
```

Después de conectar los cables entre los dos switches, este es el estado.

```
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 14 20:32:44 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4

Switch-A show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  1          normal a-full a-100 10/100BaseTX
Switch-B show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  1          normal a-full a-100 10/100BaseTX
```

Debido a que las configuraciones del switch se eliminaron antes de comenzar esta prueba, los puertos están en sus condiciones predeterminadas. Todos están en vlan1 y su velocidad y dúplex están configuradas como automáticas. Luego de conectar los cables, negocian una velocidad de 100 Mbps y dúplex completo. El estado es conectado, por lo que puede hacer ping al otro switch.

```
Switch-A ping 172.16.84.17
172.16.84.17 is alive
```

En su red, puede establecer las velocidades manualmente a 100 Mbps y dúplex completo en lugar de depender de la negociación automática, ya que probablemente desee que sus puertos funcionen siempre a la velocidad más rápida. Para ver una explicación de la negociación automática, vea la sección Resolución de Problemas de la Negociación Automática de Dúplex Completo/Medio/Medio/Medio Ethernet 10/100Mb.

Verifique que los puertos a agrupar tengan la misma configuración. Este es un punto importante que se trata con más detalle en la sección de resolución de problemas. Si el comando para configurar EtherChannel no funciona, esto generalmente es porque los puertos involucrados en el canal tienen configuraciones que difieren unas de otras. Esto incluye los puertos en el otro lado del enlace, así como también los puertos locales. En este caso, dado que las configuraciones del switch se borraron antes de que comenzara esta prueba, los puertos se encuentran en sus condiciones predeterminadas. Todos están en vlan1; su velocidad y dúplex están configurados en auto, y todos los parámetros del árbol de expansión para cada puerto están configurados de la misma manera. En la salida se vio que después de conectar los cables, los puertos negocian a una velocidad de 100 Mbps y dúplex completo. Dado que el árbol de expansión se ejecuta para cada VLAN, es más fácil configurar el canal y responder a los mensajes de error que probar y verificar la coherencia de cada campo del árbol de expansión para cada puerto y VLAN en el canal.

Identifique grupos de puertos válidos. En Catalyst 5000, solo se pueden poner juntos en un canal determinados puertos. Estas dependencias restrictivas no se aplican a todas las plataformas. Los puertos en un canal en Catalyst 5000 deben ser contiguos. Observe desde el comando **show port capabilities** que para el puerto 2/1, estas son las combinaciones posibles:

```
Switch-A show port capabilities
Model                   WS-X5225R
Port                    2/1
Channel                 2/1-2,2/1-4
```

Tenga en cuenta que este puerto puede formar parte de un grupo de dos (2/1-2) o parte de un grupo de cuatro (2/1-4). Hay algo llamado controlador de agrupación de Ethernet (EBC) en el módulo que provoca estas limitaciones de configuración. Mira otro puerto.

```
Switch-A show port capabilities 2/3
Model                   WS-X5225R
Port                    2/3
Channel                 2/3-4,2/1-4
```

Este puerto se puede agrupar en un grupo de dos puertos (2/3-4) o en un grupo de cuatro puertos (2/1-4).

Nota: Dependiendo del hardware, puede haber restricciones adicionales. En ciertos módulos

(WS-X5201 y WS-X5203), no puede conformar EtherChannel con los últimos dos puertos de un "grupo de puertos", a menos que los primeros dos puertos del grupo ya formen parte de EtherChannel. Un "grupo de puertos" es un grupo de puertos al que se le permite conformar EtherChannel (en este ejemplo, 2/1-4 es un grupo de puertos). Por ejemplo, si crea EtherChannels separados con solo dos puertos en un canal, no puede asignar los puertos 2/3-4 a un canal hasta que primero configure los puertos 2/1-2 en un canal para los módulos que tienen esta restricción. De manera similar, antes de configurar los puertos 2/6-7, debe configurar los puertos 2/5-6. Esta restricción no se produce en los módulos utilizados para este documento (WS-X5225R, WS-X5234).

Dado que configura un grupo de cuatro puertos (2/1-4), se encuentra dentro del agrupamiento aprobado. no puede asignar un grupo de cuatro a los puertos 2/3-6. Este es un grupo de puertos contiguos, pero no comienzan en el límite aprobado, como se muestra en el comando **show port capabilities** (los grupos válidos serían los puertos 1-4, 5-8, 9-12, 13-16, 17-20, 21-24).

Cree el canal Para crear el canal, utilice el **comando set port channel <mod/port on** para cada switch. se recomienda desactivar los puertos en un lado del canal o en el otro lado con el comando **set port** disable antes de activar EtherChannel manualmente. Esto evitará posibles problemas con el árbol de expansión durante el proceso de configuración. El árbol de expansión podría cerrar algunos puertos (con el estado de puerto "error desactivado") si se configura un lado como canal antes de que el otro lado se configure como tal. Debido a esta posibilidad, es mucho más sencillo crear EtherChannels utilizando el PAgP, como se explicará más adelante en este documento. Para evitar esta situación cuando configura EtherChannel manualmente, inhabilita los puertos en el SwitchA, configura el canal en el SwitchA, configura el canal en el SwitchB y luego vuelve a habilitar los puertos en el SwitchA.

Primero, verifique que la canalización *esté desactivada*.

```
Switch-A (enable) show port channel
No ports channelling
Switch-B (enable) show port channel
No ports channelling
```

Ahora, desactive los puertos en el switch A hasta que ambos switches se hayan configurado para EtherChannel de modo que el árbol de expansión no genere errores y cierre los puertos.

```
Switch-A (enable) set port disable 2/1-4
Ports 2/1-4 disabled.
[output from SwitchA upon disabling ports]
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 00:06:40 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
```

Encienda el modo de canal del conmutador A.

```
Switch-A (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
```

Verifique el estado del canal. Observe que el modo de canal se ha configurado en *on*, pero el estado de los puertos es disabled (porque usted inhabilitó entonces anteriormente). El canal no funciona en este punto, pero comenzará a funcionar cuando se activen los puertos.

```
Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  disabled   on        channel
 2/2  disabled   on        channel
 2/3  disabled   on        channel
 2/4  disabled   on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

Dado que los puertos del switch A estuvieron (temporalmente) desactivados, los puertos del switch B ya no tienen una conexión. Este mensaje aparece en la consola del switch B cuando los puertos del switch A están desactivados.

```
Switch-B (enable)
2000 Jan 13 22:30:03 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 13 22:30:04 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
```

Encienda el canal para el switch B.

```
Switch-B (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
```

Verifique que el modo de canal esté activado para el switch B.

```
Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  notconnect on        channel
 2/2  notconnect on        channel
 2/3  notconnect on        channel
 2/4  notconnect on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

Observe que el modo de canal para el SwitchB está activado, pero el estado de los puertos

noestá conectado. Esto se debe a que los puertos del SwitchA todavía están desactivados.

Finalmente, el último paso es activar los puertos en el SwitchA.

```
Switch-A (enable) set port enable 2/1-4
Ports 2/1-4 enabled.
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 15 00:08:40 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

Verifique la Configuración

Para verificar que el canal esté configurado correctamente, ejecute el comando **show port** channel.

```
Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  on        channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066509957(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066509957(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066509957(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  on        channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------
```

En este comando, se muestra cómo el árbol de expansión trata a los puertos como puertos lógicos. Cuando el puerto aparece como *2/1-4*, el spanning tree maneja los puertos 2/1, 2/2, 2/3 y 2/4 *como un puerto*.

```
Switch-A (enable) show spantree
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-10-0d-b2-8c-00
Designated Root Priority    32768
Designated Root Cost        8
Designated Root Port        2/1-4
```

```
Root Max Age   20 sec    Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-90-92-b0-84-00
Bridge ID Priority          32768
Bridge Max Age 20 sec    Hello Time 2  sec   Forward Delay 15 sec

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------- ----  -------------  -----  --------  ----------  ------------
 2/1-4    1     forwarding         8        32   disabled       channel
```

Se puede implementar EtherChannel con diferentes maneras de distribución de tráfico a través de los puertos en un canal. La especificación EtherChannel no determina cómo se debe distribuir el tráfico a través de los links en un canal. Catalyst 5000 utiliza el último bit o los dos últimos bits (según la cantidad de enlaces que haya en el canal) de las direcciones MAC de origen y destino en la trama para determinar qué puerto en el canal utilizar. Si el tráfico se genera por una distribución normal de direcciones MAC en cualquiera de los lados del canal, observará cantidades similares de tráfico en cada puerto del canal. Para verificar que el tráfico pasa por todos los puertos en el canal, puede utilizar el comando **show**. Si sus puertos estaban activos antes de configurar EtherChannel, puede restablecer los contadores de tráfico a cero mediante el comando **clear** counters, y luego los valores de tráfico representan cómo EtherChannel ha distribuido el tráfico.

En este entorno de prueba, no se obtuvo una distribución real porque no hay estaciones de trabajo, servidores o routers que generen tráfico. Los únicos dispositivos que generan tráfico son los propios switches. Usted emitió algunos pings del SwitchA al SwitchB, y puede decir que el tráfico unicast utiliza el primer puerto en el canal. La información de recepción en este caso (unidifusión Rcv) muestra cómo el Switch B distribuyó el tráfico a través del canal hasta el Switch A. Un poco más abajo en la salida, la información de transmisión (Xmit-Unicast) muestra cómo el SwitchA distribuyó el tráfico a través del canal al SwitchB. También puede ver que una pequeña cantidad de tráfico multicast generado por el switch (ISL dinámico, CDP) sale de los cuatro puertos. Los paquetes de difusión son consultas ARP (para el gateway predeterminado, que no existe aquí). Si tiene estaciones de trabajo que envían paquetes a través del switch a un destino del otro lado del canal, esperaría ver el tráfico que pasa por cada uno de los cuatro links en el canal. Puede monitorear la distribución de paquetes en su propia red con el comando **show**.

```
Switch-A (enable) clear counters
This command will reset all MAC and port counters reported in CLI and SNMP.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.
Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                      9                  320                  183
 2/2                      0                   51                    0
 2/3                      0                   47                    0
 2/4                      0                   47                    0
(...)

Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                      8                   47                  184
 2/2                      0                   47                    0
 2/3                      0                   47                    0
 2/4                      0                   47                    0
(...)
```

```
Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
 2/1                    35176                17443
 2/2                     5304                 4851
 2/3                     5048                 4851
 2/4                     5048                 4851
(...)

Last-Time-Cleared
--------------------------
Wed Dec 15 1999, 01:05:33
```

Uso del PAgP para configurar EtherChannel (método preferido)

El protocolo de agregración de puertos (PAgP) facilita la creación automática de enlaces EtherChannel mediante el intercambio de paquetes entre los puertos con capacidad de canal. El protocolo aprende dinámicamente las capacidades de los grupos de puertos e informa a los puertos cercanos.

Una vez que PAgP identifica los links channel-capable que pueden juntarse correctamente, agrupa los puertos en un canal. El canal luego se agrega al árbol de expansión como un solo puerto de puente. Un paquete de difusión o de multidifusión de salida determinado se transmite sólo a un puerto del canal y no a todos los puertos del canal. Además, la transmisión saliente y los paquetes de multidifusión transmitidos por un puerto en un canal quedan bloqueados para regresar a través de cualquier otro puerto del canal.

Hay cuatro modos de canal configurables por el usuario: on, off, auto y desirable. Los paquetes PAgP se intercambian solamente entre los puertos inautoydeseablemode. Los puertos configurados en modo inonoroffmode no intercambian paquetes PAgP. La configuración recomendada para los switches que desea formar y EtherChannel es tener ambos switches configurados en modo deseable. Esto proporciona el comportamiento más robusto cuando un lado u otro encuentran situaciones de error o se restablecen. El modo predeterminado del canal es **auto**.

Tanto los modos automáticos como deseables permiten que los puertos negocien con los puertos conectados para determinar si pueden formar un canal en función de criterios como la velocidad del puerto, el estado del enlace troncal, la VLAN nativa, etc.

Los puertos pueden conformar EtherChannel cuando están en diferentes modos de canal, siempre que los modos sean compatibles.

Un puerto indesirablemode puede formar un EtherChannel exitosamente con otro puerto que es indesirableorautomode.

Un puerto inautomode puede formar un EtherChannel con otro puerto indesirablemode.

Un puerto inautomode no puede formar un EtherChannel con otro puerto que también esté inautomode ya que ninguno de los dos puertos inicia la negociación.

Un puerto inonmode puede formar un canal sólo con un puerto inonmode porque los puertos inonmode no intercambian paquetes PAgP.

Un puerto inoffmode no forma un canal con ningún puerto.

Cuando utiliza EtherChannel, si se muestra un mensaje "SPANTREE-2: Channel misconfig - x/x-x will be disabled" o similar de syslog, indica una discordancia de los modos EtherChannel en los puertos conectados. le recomienda que corrija la configuración y vuelva a habilitar los puertos con el comando **set port** enable. Las configuraciones válidas de EtherChannel incluyen las siguientes:

Tabla 22-5: Configuraciones EtherChannel válidas

Modo de canal de puerto	Modo(s) de canal del puerto de vecino válido(s)
deseable	deseable o automático
Automática (predeterminada)	deseable o automático1
encendido	encendido
desactivado	desactivado

[1]Si los puertos locales y vecinos están en modo automático, no se forma un conjunto EtherChannel.

Este es un resumen de todas las situaciones posibles del modo de canalización. Algunas de estas combinaciones pueden hacer que el spanning tree coloque los puertos del lado de canalización en estado errdisable (es decir, los apague).

Tabla 22-6: Escenarios del modo de canalización

Modo de Canal de Switch-A	Modo de Canal del Switch B	Estado del Canal
Encendido	Encendido	Canal
Encendido	Desactivado	Sin canal (error desactivado)
Encendido	Auto	Sin canal (error desactivado)
Encendido	Deseable	Sin canal (error desactivado)
Desactivado	Encendido	Sin canal (error desactivado)
Desactivado	Desactivado	Sin Canal
Desactivado	Auto	Sin Canal
Desactivado	Deseable	Sin Canal
Auto	Encendido	Sin canal (error desactivado)
Auto	Desactivado	Sin Canal
Auto	Auto	Sin Canal
Auto	Deseable	Canal
Deseable	Encendido	Sin canal (error desactivado)
Deseable	Desactivado	Sin Canal
Deseable	Auto	Canal
Deseable	Deseable	Canal

Apagó el canal del ejemplo anterior con este comando en el SwitchA y el SwitchB.

```
Switch-A (enable) set port channel 2/1-4 auto
Port(s) 2/1-4 channel mode set to auto.
```

El modo de canal predeterminado de un puerto capaz de canalizar es automático. Para verificar esto, ingrese este comando:

```
Switch-A (enable) show port channel 2/1
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  auto      not channel
```

El comando anterior muestra asimismo que actualmente los puertos no se canalizan. Otra forma de verificar el estado del canal es esta.

```
Switch-A (enable) show port channel
No ports channelling
Switch-B (enable) show port channel
No ports channelling
```

Es muy simple hacer que el canal funcione con el PAgP. En ese momento, ambos switches están configurados en el modo automático, lo que significa que van a formar un mismo canal si un puerto que está conectado envía una solicitud de PAgP para canalizarse. Si configura el SwitchA como deseable, el SwitchA, hace que el SwitchA envíe paquetes PAgP al otro switch y le pide que canalice.

```
Switch-A (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 22:03:18 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 15 22:03:19 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 15 22:03:19 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 15 22:03:20 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 15 22:03:23 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 15 22:03:24 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4
```

Para ver el canal, haga esto.

```
Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  desirable channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  desirable channel     WS-C5505    066509957(Sw  2/2
 2/3  connected  desirable channel     WS-C5505    066509957(Sw  2/3
 2/4  connected  desirable channel     WS-C5505    066509957(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------
```

Debido a que el switch B está en el modo automático, responde a los paquetes PAgP y crea un canal con el switch A.

```
Switch-B (enable)
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/1 left bridg1
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 14 20:26:41 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 14 20:26:45 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 14 20:26:47 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 14 20:26:48 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  auto      channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  auto      channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  auto      channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  auto      channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------
```

Nota: Se recomienda configurar ambos lados del canal a deseable para que ambos lados intenten iniciar el canal si uno de los lados se cae. Si configura los puertos EtherChannel en el SwitchB en el modo deseable, aunque el canal esté actualmente activo e inautomode, no plantea ningún problema. Este es el comando.

```
Switch-B (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  desirable channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  desirable channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  desirable channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  desirable channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------
```

Ahora, si el switch A deja de funcionar por alguna razón o si un hardware nuevo reemplaza a ese switch, el switch B tratará de reestablecer el canal. Si el nuevo equipo no puede establecer el canal, el switch B tratará a sus puertos 2/1-4 como puertos normales de no canalización. Esta es una de las ventajas del uso del mododeseable. Si el canal se configuró utilizando el modo PAgP activado y un lado de la conexión tiene un error de cualquier tipo o un reinicio, podría provocar un estado de error desactivado (apagado) en el otro lado. Con el PAgP establecido en el modo deseado en cada lado, el canal estabiliza y renegocia la conexión de EtherChannel.

Enlace troncal y EtherChannel

EtherChannel es independiente del enlace troncal. Puede activar los enlaces troncales o dejar los enlaces troncales desactivados. También puede activar el enlace troncal para todos los puertos antes de crear el canal, o puede activarlo después de crear el canal (como hace aquí). En lo que

respecta a EtherChannel, no importa; el trunking y EtherChannel son funciones completamente separadas. Lo que importa es que todos los puertos involucrados estén en el mismo modo: o bien todos ellos son enlaces troncales antes de configurar el canal, o bien no son enlaces troncales antes de configurar el canal. Todos los puertos deben estar en el mismo estado troncal antes de crear el canal. Una vez que se forma una canal, todo lo que se cambie en un puerto también se cambia para los otros puertos en el canal. Los módulos que se utilizan en este banco de pruebas pueden realizar enlaces troncales ISL o 802.1q. De manera predeterminada, los módulos se establecen en el modo de enlace troncal automático y negociación, lo que significa que son enlaces troncales si el otro lado les solicita el enlace troncal y negocian si deben utilizar el método ISL o 802.1q para el enlace troncal. Si no se les solicita el enlace troncal, funcionan como puertos normales que no son enlaces troncales.

```
Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         negotiate      not-trunking  1
 2/2      auto         negotiate      not-trunking  1
 2/3      auto         negotiate      not-trunking  1
 2/4      auto         negotiate      not-trunking  1
```

Existen diversas formas de activar los enlaces troncales. En este ejemplo, se establece SwitchA en desirable. El SwitchA ya está configurado para negociar. La combinación deseable/negociación hace que el switch A solicite al switch B el enlace troncal y negocie el tipo de conformación de enlaces troncales (ISL o 802.1q). Dado que el switch B se establece de manera predeterminada para la negociación automática, el switch B responde a la solicitud del switch A. Se producen los siguientes resultados:

```
Switch-A (enable) set trunk 2/1 desirable
Port(s) 2/1-4 trunk mode set to desirable.
Switch-A (enable)
1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/1 has become isl trunk
1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/2 has become isl trunk
1999 Dec 18 20:46:25 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
1999 Dec 18 20:46:25 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
1999 Dec 18 20:46:25 %DTP-5-TRUNKPORTON:Port 2/3 has become isl trunk
1999 Dec 18 20:46:26 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
1999 Dec 18 20:46:26 %DTP-5-TRUNKPORTON:Port 2/4 has become isl trunk
1999 Dec 18 20:46:26 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4
1999 Dec 18 20:46:28 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
1999 Dec 18 20:46:29 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      desirable    n-isl          trunking      1
 2/2      desirable    n-isl          trunking      1
 2/3      desirable    n-isl          trunking      1
 2/4      desirable    n-isl          trunking      1
```

El modo de enlace troncal se configuró como deseable. El resultado fue que el modo de trunking fue negociado con el switch vecino y decidieron usar ISL (**n-isl**). El estado actual ahora es **trunking** . Esto sucede en el switch B debido a la ejecución del comando en el switch A.

```
Switch-B (enable)
```

```
2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/1 has become isl trunk
2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/2 has become isl trunk
2000 Jan 17 19:09:52 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
2000 Jan 17 19:09:52 %DTP-5-TRUNKPORTON:Port 2/3 has become isl trunk
2000 Jan 17 19:09:52 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
2000 Jan 17 19:09:53 %DTP-5-TRUNKPORTON:Port 2/4 has become isl trunk
2000 Jan 17 19:09:53 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
2000 Jan 17 19:09:53 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 19:09:55 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         n-isl          trunking      1
 2/2      auto         n-isl          trunking      1
 2/3      auto         n-isl          trunking      1
 2/4      auto         n-isl          trunking      1
```

Observe que los cuatro puertos (2/1-4) se convirtieron en troncales, aunque solo haya cambiado específicamente un puerto (2/1) a desirable. Este es un ejemplo de cómo el cambio de un puerto en el canal afecta a todos los puertos.

Troubleshooting de EtherChannel

Los desafíos para EtherChannel se pueden dividir en dos áreas principales: resolver el problema dentro de la fase de configuración y resolver el problema dentro de la fase de ejecución. Los errores de configuración generalmente ocurren debido a parámetros no coincidentes en los puertos involucrados (diferentes velocidades, diferentes dúplex, diferentes valores de puerto de árbol de expansión, etc.). También puede generar errores dentro de la configuración si configura el canal en un lado y espera demasiado antes de configurar el canal en el otro lado. Esto causa bucles en el árbol de expansión, lo que genera un error y apaga el puerto.

Cuando encuentre un error mientras se configura EthernetChannel, asegúrese de controlar el estado de los puertos luego de corregir la situación de error de EtherChannel. Si el estado del puerto es *serrdisable*, significa que los puertos han sido apagados por el software y no se vuelven a encender hasta que ingresa el comando **set port** enable.

Nota: Si el estado del puerto *se vuelve errdisable*, debe habilitar específicamente los puertos con el comando **set port** enable para que los puertos se vuelvan activos. Actualmente, puede corregir todos los problemas de EtherChannel, pero los puertos no se activan ni forman un canal hasta que se activan nuevamente. Las versiones futuras del sistema operativo pueden comprobar periódicamente si se deben habilitar los puertos que se pueden deshabilitar.

Para estas pruebas usted desactiva el trunking y EtherChannel: Parámetros no coincidentes; Espere demasiado tiempo antes de configurar el otro lado; Corrija el estado errdisable; y muestre lo que sucede cuando un link se rompe y se restaura.

Parámetros no coincidentes

Este es un ejemplo de parámetros no coincidentes. Usted configura el puerto 2/4 en la VLAN 2 mientras que los otros puertos todavía están en la VLAN 1. Para crear una nueva VLAN, debe asignar un dominio VTP para el switch y crear la VLAN.

```
Switch-A (enable) show port channel
No ports channelling

Switch-A (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  1          normal a-full a-100 10/100BaseTX

Switch-A (enable) set vlan 2
Cannot add/modify VLANs on a VTP server without a domain name.

Switch-A (enable) set vtp domain testDomain
VTP domain testDomain modified

Switch-A (enable) set vlan 2 name vlan2
Vlan 2 configuration successful

Switch-A (enable) set vlan 2 2/4
VLAN 2 modified.
VLAN 1 modified.
VLAN  Mod/Ports
----  ----------------------
2     2/4

Switch-A (enable)
1999 Dec 19 00:19:34 %PAGP-5-PORTFROMSTP:Port 2/4 left bridg4

Switch-A (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  2          normal a-full a-100 10/100BaseTX

Switch-A (enable) set port channel 2/1-4 desirable
Port(s) 2/1-4 channel mode set to desirable.

Switch-A (enable)
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 19 00:20:19 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:20:20 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:20:20 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
1999 Dec 19 00:20:22 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:20:22 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:20:24 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-2
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-2
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 19 00:20:25 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4

Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  desirable channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  desirable channel     WS-C5505    066509957(Sw  2/2
----- ---------- --------- ----------- ------------------------- ----------
```

Observe que el canal se formó solo entre los puertos 2/1-2. Se dejaron afuera los puertos 2/3-4

porque el puerto 2/4 estaba en una VLAN diferente. No hubo mensaje de error; PAgP simplemente hizo lo que pudo para hacer que el canal funcionara. es necesario observar los resultados cuando se crea el canal para asegurarse de que hizo lo que deseaba.

Ahora configure el canal manualmente en "on" con el puerto 2/4 en una VLAN diferente y vea qué sucede. En primer lugar, vuelva a establecer el modo de canal en auto para cerrar el canal actual, luego configure el canal manualmente en "on".

```
Switch-A (enable) set port channel 2/1-4 auto
Port(s) 2/1-4 channel mode set to auto.
Switch-A (enable)
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-2
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-2
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
1999 Dec 19 00:26:08 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
1999 Dec 19 00:26:18 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
1999 Dec 19 00:26:19 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/4

Switch-A (enable) show port channel
No ports channelling

Switch-A (enable) set port channel 2/1-4 on
Mismatch in vlan number.
Failed to set port(s) 2/1-4 channel mode to on.

Switch-A (enable) show port channel
No ports channelling
```

En el SwitchB puede encender el canal y notar que dice que el canal de los puertos está bien, pero sabe que el SwitchA no está configurado correctamente.

```
Switch-B (enable) show port channel
No ports channelling

Switch-B (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal a-full a-100 10/100BaseTX
 2/2                     connected  1          normal a-full a-100 10/100BaseTX
 2/3                     connected  1          normal a-full a-100 10/100BaseTX
 2/4                     connected  1          normal a-full a-100 10/100BaseTX

Switch-B (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.

Switch-B (enable)
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/2
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
2000 Jan 17 22:54:59 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 22:55:00 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
```

```
Port  Status     Channel   Channel     Neighbor                 Neighbor
                 mode      status      device                   port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  connected  on        channel     WS-C5505    066507453(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066507453(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066507453(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066507453(Sw  2/4
----- ---------- --------- ----------- ------------------------ ----------
```

Esto clarifica que usted debe verificar ambos lados del canal al configurarlo manualmente para asegurarse de que ambos lados estén activos y no solo uno de ellos. Este resultado muestra que el switch B está configurado para un canal, pero este no está canalizando porque posee un puerto que se encuentra en la VLAN incorrecta.

Esperó demasiado para configurar el otro lado

En esta situación, el Switch B tiene el EtherChannel encendido, pero el Switch A no porque tiene un error de configuración de VLAN (los puertos 2/1-3 están en vlan1, el puerto 2/4 está en vlan2). Esto es lo que sucede cuando un lado de EtherChannel se establece en activado y el otro lado aún está en modo automático. El switch B, luego de unos minutos, apaga sus puertos dado que detecta un bucle de expansión. Esto se produce debido a que los puertos 2/1-4 del Switch B se comportan como si fueran un único puerto grande, mientras que los puertos 2/1-4 del Switch B son puertos totalmente independientes. Una transmisión enviada desde el switch B al switch A en el puerto 2/1 se reenviará al switch B en los puertos 2/2, 2/3 y 2/4, ya que el switch A trata estos puertos como independientes. Esta es la razón por la que el SwitchB informa que hay un loop de spanning tree. Observe que los puertos en el SwitchB ahora están inhabilitados y tienen un estado *oferrdisable*.

```
Switch-B (enable)
2000 Jan 17 22:55:48 %SPANTREE-2-CHNMISCFG: STP loop - channel 2/1-4 is disabled in vlan 1.
2000 Jan 17 22:55:49 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4
2000 Jan 17 22:56:01 %PAGP-5-PORTFROMSTP:Port 2/2 left bridge port 2/1-4
2000 Jan 17 22:56:13 %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/1-4
2000 Jan 17 22:56:36 %PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                 Neighbor
                 mode      status      device                   port
----- ---------- --------- ----------- ------------------------ ----------
 2/1  errdisable on        channel
 2/2  errdisable on        channel
 2/3  errdisable on        channel
 2/4  errdisable on        channel
----- ---------- --------- ----------- ------------------------ ----------
Switch-B (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     errdisable 1          normal   auto  auto 10/100BaseTX
 2/2                     errdisable 1          normal   auto  auto 10/100BaseTX
 2/3                     errdisable 1          normal   auto  auto 10/100BaseTX
 2/4                     errdisable 1          normal   auto  auto 10/100BaseTX
```

Corrección del estado de error desactivado

A veces, cuando intenta configurar EtherChannel, pero los puertos no están configurados de la misma manera, hace que los puertos de un lado del canal o del otro se apaguen. Las luces de enlace son amarillas en el puerto. Puede ver esto en la consola si escribe **show port**. Los puertos se enumeran *aserrdisable*. Para poder recuperarse de esto, debe reparar los parámetros que no

coinciden en los puertos involucrados y, luego, volver a habilitar los puertos. Tenga en cuenta que esta rehabilitación de los puertos es un paso independiente que debe realizarse para que los puertos vuelvan a ser funcionales.

En este ejemplo, sabe que el SwitchA tenía una discordancia de vlan. Vaya al SwitchA y vuelva a colocar el puerto 2/4 en vlan1. Luego activa el canal para los puertos 2/1-4. El switch A no se muestra conectado hasta que se vuelven a habilitar los puertos del switch B. Luego, cuando haya corregido el SwitchA y lo haya puesto en modo de canalización, vuelva al SwitchB y vuelva a habilitar los puertos.

```
Switch-A (enable) set vlan 1 2/4
VLAN 1 modified.
VLAN 2 modified.
VLAN  Mod/Ports
---- ----------------------
1     2/1-24

Switch-A (enable) set port channel 2/1-4 on
Port(s) 2/1-4 channel mode set to on.
Switch-A (enable) sh port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  notconnect on        channel
 2/2  notconnect on        channel
 2/3  notconnect on        channel
 2/4  notconnect on        channel
----- ---------- --------- ----------- ------------------------- ----------

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  errdisable on        channel
 2/2  errdisable on        channel
 2/3  errdisable on        channel
 2/4  errdisable on        channel
----- ---------- --------- ----------- ------------------------- ----------

Switch-B (enable) set port enable 2/1-4
Ports 2/1-4 enabled.
Switch-B (enable) 2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/1 joined bridg4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/1-4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/1-4
2000 Jan 17 23:15:22 %PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/1-4

Switch-B (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  on        channel
 2/2  connected  on        channel
 2/3  connected  on        channel
 2/4  connected  on        channel
----- ---------- --------- ----------- ------------------------- ----------
```

Qué sucede cuando un enlace se interrumpe y restaura

Cuando un puerto en el canal se desactiva, los paquetes que se enviarían normalmente por ese

puerto se envían por el próximo puerto en el canal. Puede verificar que esto sucede con el comando **show**. En este banco de pruebas, el SwitchA envía paquetes de ping al SwitchB para ver qué link utiliza el tráfico. Primero borra los contadores, luego muestra mac, envía tres pings y **luego muestra** macagain para ver en qué canal se recibieron las respuestas de ping.

```
Switch-A (enable) clear counters
This command will reset all MAC and port counters reported in CLI and SNMP.
Do you want to continue (y/n) [n]? y
MAC and Port counters cleared.

Switch-A (enable) show port channel
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  on        channel     WS-C5505    066509957(Sw  2/1
 2/2  connected  on        channel     WS-C5505    066509957(Sw  2/2
 2/3  connected  on        channel     WS-C5505    066509957(Sw  2/3
 2/4  connected  on        channel     WS-C5505    066509957(Sw  2/4
----- ---------- --------- ----------- ------------------------- ----------

Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                      0                   18                    0
 2/2                      0                    2                    0
 2/3                      0                    2                    0
 2/4                      0                    2                    0
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                      3                   24                    0
 2/2                      0                    2                    0
 2/3                      0                    2                    0
 2/4                      0                    2                    0
```

En este momento, ha recibido las respuestas de ping en el puerto 3/1. Cuando la consola del switch B envía una respuesta al switch A, EtherChannel utiliza el puerto 2/1. Ahora apaga el puerto 2/1 en el SwitchB. Desde el SwitchA usted emite otro ping y ve en qué canal se reactiva la respuesta. (El SwitchA envía en el mismo puerto al que está conectado el SwitchB. Usted sólo muestra los paquetes recibidos del SwitchB porque los paquetes de transmisión están más abajo en **la visualización de la** macro).

```
1999 Dec 19 01:30:23 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1-4

Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
```

```
 2/1                     3                  37                  0
 2/2                     1                  27                  0
 2/3                     0                   7                  0
 2/4                     0                   7                  0
```

Ahora que el puerto 2/1 está deshabilitado, EtherChannel utiliza automáticamente el siguiente puerto en el canal: 2/2. Ahora, vuelva a habilitar el puerto 2/1 y espere a que se una al grupo de puentes. A continuación, ejecute dos pings más.

```
1999 Dec 19 01:31:33 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1-4

Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) ping 172.16.84.17
172.16.84.17 is alive
Switch-A (enable) show mac

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 2/1                     5                  50                  0
 2/2                     1                  49                  0
 2/3                     0                  12                  0
 2/4                     0                  12                  0
```

Tenga en cuenta que estos pings se envían desde el puerto 2/1. Cuando el enlace vuelve a aparecer, EtherChannel lo agrega al paquete y lo utiliza. Todo esto se realiza en modo transparente para el usuario.

Comandos utilizados en esta sección

Estos son los comandos que se utilizaron en esta sección.

Comandos para utilizar para la configuración

set port channel on: activa la función EtherChannel.

set port channel auto: restablece los puertos al modo automático predeterminado.

set port channel desirable- para enviar paquetes PAgP a las solicitudes del otro lado para que se cree un canal.

set port enable: habilita los puertos después de configurar la deshabilitación de puertos o después del estado de error desactivado.

set port disable- para inhabilitar un puerto mientras se realizan otras configuraciones.

set trunk desirable: habilita el enlace troncal y hace que este puerto envíe una petición al otro switch indicando que éste es un enlace troncal. Si el puerto está configurado en negociación (configuración predeterminada), negocia el tipo de enlace troncal que se usará en el enlace (ISL o 802.1q).

Comandos para verificar la configuración

show version: muestra qué versión del software ejecuta el switch.

show module: muestra los módulos instalados en el switch.

show port capabilities- para determinar si los puertos que desea utilizar tienen la capacidad de hacer EtherChannel.

show port - para determinar el estado del puerto (desconectado, conectado) y las configuraciones de dúplex y de velocidad.

ping : prueba la conectividad con el otro switch.

show port channel - Para ver el estado actual del agrupamiento de EtherChannel.

show port channel mod/port: brinda una vista más detallada del estado del canal de un solo puerto.

show spantree – para comprobar que el árbol de expansión detectó el canal como un link.

show trunk - para ver el estado de conexión troncal de los puertos.

Comandos para usar para la resolución de problemas de configuración

show port channel - Para ver el estado actual del agrupamiento de EtherChannel.

show port - para determinar el estado del puerto (desconectado, conectado) y las configuraciones de dúplex y de velocidad.

clear counters - para reiniciar los contadores de paquete del switch a cero. Los contadores son visibles con el comando show.

show mac: brinda una vista de los paquetes recibidos y enviados por el switch.

ping: para probar la conectividad con el otro switch y generar el tráfico que aparece con el comando show mac.

Utilice Portfast y Otros Comandos para Solucionar Problemas de Conectividad de Inicio de Estación Final

Si tiene estaciones de trabajo conectadas a switches que no pueden iniciar sesión en su dominio de red (NT o Novell), o no pueden obtener una dirección DHCP, puede probar las sugerencias enumeradas en este documento antes de explorar otras vías. Las sugerencias son relativamente fáciles de implementar y muy a menudo son la causa de los problemas de conectividad de la estación de trabajo encontrados a través de la fase de inicialización/inicio de la estación de trabajo.

Con cada vez más usuarios que implementan el switching en el escritorio y reemplazan sus hubs compartidos por switches, a menudo se observan problemas que se introducen en los entornos cliente/servidor debido a este retraso inicial. El mayor problema que ve es que los clientes Windows 95/98/NT, Novell, VINES, IBM NetworkStation/IBM Thin Clients y AppleTalk no pueden conectarse a sus servidores. Si el software en estos dispositivos no es persistente dentro del procedimiento de inicio, ya no intentan conectarse a su servidor antes incluso de que el switch haya permitido el paso del tráfico.

Nota: Este retraso de conectividad inicial se manifiesta a menudo como errores que aparecen cuando inicia por primera vez una estación de trabajo. Estos son varios ejemplos de mensajes de error y errores que pueden aparecer:

- Un cliente de redes de Microsoft indica que: "No hay controladores de dominio disponibles".
- DHCP indica que: "No hay servidores DHCP disponibles".
- Una estación de trabajo de interconexión Novell IPX no muestra la pantalla "Novell Login Screen" al inicio.
- Un cliente de la red AppleTalk indica que: "El acceso a la red AppleTalk ha sido interrumpido. Para reestablecer la conexión, debe abrir y cerrar el panel de control de AppleTalk". También es posible que la aplicación Selector de cliente de AppleTalk no muestre una lista de zonas o muestre una lista de zonas incompleta.

El retardo de conectividad inicial también se observa con frecuencia en un entorno conmutado en el cual un administrador de red actualiza el software o los controladores. En este caso, un proveedor puede optimizar los controladores de modo que los procedimientos de inicialización de la red ocurran antes en el proceso de inicio del cliente (antes de que el switch esté listo para procesar los paquetes).

Con las distintas características que se incluyeron en algunos switches, en casi un minuto un switch podrá comenzar a atender a una estación de trabajo conectada recientemente. Esta demora puede afectar a la estación de trabajo cada vez que ésta se encienda o reinicie. Estas son las cuatro características principales que generan este retardo:

- Protocolo de árbol de expansión (STP)
- Negociación EtherChannel
- Negociación de enlaces troncales

Negociación de velocidad de link/dúplex entre el switch y la estación de trabajo

Las cuatro funciones figuran ordenadas de mayor retraso causado (STP) a menor retraso causado (velocidad/negociación dúplex). Una estación de trabajo conectada a un switch usualmente no causa bucles de árbol de expansión, no necesita EtherChannel ni tampoco negociar un método de concentración de enlaces. (Al desactivar la velocidad de enlace/negociación de la detección, puede también reducir el retardo del puerto si necesita optimizar el tiempo de inicio tanto como sea posible).

Esta sección muestra cómo implementar comandos de optimización de la velocidad de inicio en tres plataformas de switch Catalyst. En las secciones de temporización, usted muestra cómo se reduce la demora del puerto del switch y en qué medida.

Contenido

Los términos “estación de trabajo”, “estación extrema”, “servidor” se utilizan indistintamente en esta sección. A lo que se refiere es a cualquier dispositivo conectado directamente a un switch mediante una sola tarjeta NIC. También podemos referirnos a dispositivos con varias NIC, donde la NIC solo se utiliza para la redundancia; es decir, la estación de trabajo o el servidor no están configurados para funcionar como puente, solo tienen varias NIC para la redundancia.

Nota: Hay algunas tarjetas NIC de servidor que soportan trunking y/o EtherChannel. Hay situaciones en que el servidor debe funcionar en varias VLAN a la vez (enlace troncal) o requiere un ancho de banda mayor en el enlace que lo conecta con el switch (EtherChannel). En tales casos, no apague el PAgP ni desactive el trunking. Asimismo, estos dispositivos rara vez se apagan o reinician. Las instrucciones que contiene este documento no se aplican a este tipo de dispositivos.

Background

Esta sección cubre cuatro funciones que algunos switches poseen y que causan retrasos iniciales cuando un dispositivo se conecta a un switch. Generalmente, una estación de trabajo no causa el problema del spanning tree (loops), o no necesita la función (PAgP, DTP), por lo que el retraso es innecesario.

Spanning Tree

Si recientemente ha empezado a pasar del entorno de un concentrador a un entorno de switches, pueden aparecer estos problemas de conectividad porque un switch funciona de manera muy diferente del concentrador. Un switch proporciona conectividad en la capa de enlace de datos, no en la capa física. El switch tiene que usar un algoritmo de conexión en puente para decidir si los paquetes recibidos en un puerto necesitan transmitirse a otros puertos. El algoritmo de conexión en puente es susceptible a loops físicos en la topología de red. Debido a esta susceptibilidad a los bucles, los switches ejecutan un protocolo denominado protocolo de árbol de expansión (STP) que hace que los bucles se eliminen en la topología. Cuando se ejecuta STP hace que todos los puertos que se incluyen en el proceso de spanning tree se activen mucho más lentamente de lo que lo harían de otra manera, ya que detecta y bloquea los loops. Una red conectada mediante un puente que tiene bucles físicos se romperá sin un árbol de expansión. A pesar del tiempo implicado, el STP es algo bueno. El árbol de expansión que se ejecuta en lo switches Catalyst es una especificación estándar de la industria (IEEE 802.1d).

Luego de que un puerto en el switch se haya unido al grupo puente, ejecutará el árbol de expansión en ese puerto. Un puerto que ejecuta spanning tree puede tener 1 de 5 estados: bloqueo, escucha, aprendizaje, reenvío y deshabilitado. El árbol de expansión indica que el puerto inicia el bloqueo y, luego, pasa rápidamente a las fases de escucha y aprendizaje. De forma predeterminada, pasa aproximadamente 15 segundos escuchando y 15 segundos aprendiendo.

Durante el estado de escucha, el switch trata de determinar a qué parte de la topología del árbol de expansión pertenece. Quiere saber, especialmente, si este puerto es parte de un bucle físico o no. Si forma parte de un bucle, este puerto puede elegirse para entrar en el modo de bloqueo. El bloqueo significa que no envía ni recibe datos de usuario para eliminar bucles. Si el puerto no forma parte de un bucle, continúa con el estado de aprendizaje, lo que implica aprender qué direcciones MAC se desconectan de este puerto. Todo este proceso de inicialización del árbol de expansión tarda alrededor de 30 segundos.

Si conecta una estación de trabajo o un servidor con una sola NIC a un puerto de conmutación, esta conexión no podrá crear un bucle físico. Se considera que estas conexiones son nodos hoja. No hay razón para hacer esperar 30 segundos a la estación de trabajo mientras el switch verifica la presencia de loops cuando la estación de trabajo no puede provocar un loop. Por lo tanto, Cisco agregó una función llamada "Portfast" o "Fast-Start", que significa que el spanning tree para este puerto puede asumir que el puerto no es parte de un loop y puede pasar inmediatamente al estado de reenvío, y omitir los estados de bloqueo, escucha o aprendizaje. Esto puede ahorrar mucho tiempo. Este comando no desactiva el árbol de expansión. Simplemente, hace que el árbol de expansión en el puerto seleccionado saltee algunos pasos (innecesarios en este caso) al principio.

Nota: La función Portfast nunca se debe utilizar en puertos de switch que se conectan a otros switches, hubs o routers. Estas conexiones pueden causar bucles físicos y es muy importante que el árbol de expansión pase por el procedimiento de inicialización completo en estas situaciones. Un loop de spanning tree puede interrumpir el funcionamiento de su red. Si se activa PortFast para un puerto que forma parte de un bucle físico, puede producirse una ventana de tiempo en la que los paquetes puedan reenviarse continuamente (e incluso multiplicar) de tal manera que la red no pueda recuperarse. En el software posterior del sistema operativo Catalyst (5.4(1)), existe una función denominada Protección de la BPDU de PortFast, que detecta la recepción de BPDU

en los puertos que tienen PortFast activado. Dado que esto no debería ocurrir, la protección de BPDU coloca el puerto en el estado "error desactivado".

EtherChannel

Otra función con la que puede contar un switch se denomina EtherChannel (o Fast EtherChannel o Gigabit EtherChannel). Esta función permite que enlaces múltiples entre los mismos dos dispositivos operen como si fueran un único enlace rápido con una carga de tráfico equilibrada entre los enlaces. Un switch puede formar estas agrupaciones automáticamente con un vecino mediante un protocolo llamado protocolo de agregación de puertos (PAgP). Los puertos de switch que pueden ejecutar el PAgP generalmente tienen un modo pasivo predeterminado llamado "automático", lo que significa que pueden formar un paquete si el dispositivo vecino lo solicita a través del enlace. Si se ejecuta el protocolo en el modo automático, puede provocar que el puerto tenga una demora de hasta 15 segundos antes de pasar el control al algoritmo de árbol de expansión (el PAgP se ejecuta en un puerto antes que el árbol de expansión). No existen motivos para que el PagP se ejecute en un puerto conectado a una estación de trabajo. Si "desactiva" el modo PAgP del puerto del switch, se eliminará este retardo.

Trunking

Otra característica del switch es la capacidad que posee un puerto de formar una troncal. Cuando se necesita transportar el tráfico desde las Redes virtuales de área local (VLAN), se configura un tronco entre dos dispositivos. Los switches crean una VLAN para hacer que un grupo de estaciones de trabajo aparenten estar en su propio "segmento" o "dominio de transmisión". Los puertos troncales hacen que estas VLAN se extiendan por múltiples switches, de modo que una única VLAN pueda cubrir una oficina central completa. Lo hacen con la adición de etiquetas a los paquetes; esto indica a qué VLAN pertenece el paquete.

Existen diversos tipos de protocolos trunking. Si un puerto puede convertirse en un enlace troncal, también puede tener la capacidad de restringir automáticamente, y en algunos casos incluso de negociar, qué tipo de enlace troncal se debe utilizar en el puerto. Esta capacidad de negociar el método de conexión troncal con el otro dispositivo se denomina Protocolo de concentración de enlaces dinámico (DTP), cuyo precursor es un protocolo denominado ISL dinámico (DISL). Si estos protocolos se ejecutan, pueden retrasar un puerto en el switch que se vuelve activo.

Por lo general, un puerto conectado a una estación de trabajo pertenece a una sola VLAN y, por lo tanto, no necesita conectarse a un trunk. Generalmente, si un puerto está capacitado para negociar la formación de un enlace troncal, pasará de forma predeterminada al modo "automático". Si el puerto se cambia a un modo de trunking de "apagado", reduce aún más el retraso de un puerto de switch que se vuelve activo.

Negociación de velocidad y dúplex

Todo lo que necesita hacer es encender Portfast y apagar PAgP (si está presente) para resolver el problema, pero si necesita eliminar cada segundo posible también podría configurar la velocidad del puerto y el dúplex manualmente en el switch si es un puerto de múltiples velocidades (10/100). La negociación automática es una buena función, pero si la apaga podría ahorrar 2 segundos en un Catalyst 5000 (no ayuda mucho en el 2800 o 2900XL).

Puede haber complicaciones, sin embargo, si apaga la negociación automática en el switch pero la deja activa en la estación de trabajo. Dado que el switch no negocia con el cliente, el cliente puede elegir la misma configuración dúplex que utiliza o no el switch. Consulte "Troubleshooting de Negociación Automática de Dúplex Medio/Medio/Completo Ethernet 10/100Mb" para obtener información adicional sobre las advertencias de la negociación automática.

Cómo reducir el retardo de inicialización en el switch Catalyst 4000/5000/6000

Estos cinco comandos muestran cómo activar Portfast, cómo desactivar la negociación PAgP, desactivar la negociación de trunking (DISL, DTP) y desactivar la negociación de velocidad/dúplex. **El** comando **set spantree portfast** se ejecuta en un rango de puertos a la vez (**set spantree portfast 2/1-12 enable**). **Generalmente,** el canal de **puerto configurado** debe desactivarse con un grupo válido de puertos con capacidad de canal. En este caso, el módulo dos tiene la capacidad de establecer un canal con los puertos 2/1-2 o con los puertos 2/1-4, por lo que cualquiera de estos grupos de puertos habría sido válido para usar.

Nota: La versión 5.2 de Cat OS para Catalyst 4000/5000 tiene un nuevo comando **llamado set port** hostque es una macro que combina estos comandos en un comando fácil de usar (excepto que no cambia la configuración de velocidad y dúplex).

Configuración

```
Switch-A (enable) set spantree portfast 2/1 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.
Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.

Switch-A (enable) set trunk 2/1 off
Port(s) 2/1 trunk mode set to off.
```

Los cambios en la configuración se guardan automáticamente en NVRAM.

Verificación

La versión de software de switch que se utiliza en este documento es 4.5(1). Para el resultado total de los comandos show version y show module, consulte la sección de prueba de sincronización.

```
Switch-A (enable) show version
WS-C5505 Software,
Version McpSW: 4.5(1) NmpSW: 4.5(1)
```

Este comando muestra cómo ver el estado actual de un puerto con respecto al árbol de expansión. Actualmente, el puerto se encuentra en el estado de reenvío del árbol de expansión (envío y recepción de paquetes) y la columna Fast-Start muestra que PortFast está actualmente deshabilitado. En otras palabras, el puerto puede tardar al menos 30 segundos en pasar al estado de reenvío cada vez que se inicializa.

```
Switch-A (enable) show port spantree 2/1

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------  ----  -------------  -----  --------  ----------  ------------
 2/1      1     forwarding        19        32
disabled
```

Ahora activa portfast en este puerto del switch. El switch nos advierte que este comando sólo debe utilizarse en puertos que estén conectados a un único host (una estación de trabajo, un servidor, etc.) y nunca en puertos conectados a otros hubs o switches. La razón por la que habilita portfast es que el puerto comienza a reenviarse inmediatamente. Puede hacer esto porque una estación de trabajo o un servidor no causa un loop de red. Esto puede hacer perder el tiempo. Sin embargo, otro concentrador o switch puede provocar un loop y usted desea pasar siempre por las etapas normales de escucha y aprendizaje cuando se conecta a estos tipos de dispositivos.

```
Switch-A (enable) set spantree portfast 2/1 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host.  Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.
```

Para verificar que PortFast esté habilitado para este puerto, ejecute este comando.

```
Switch-A (enable) show port spantree 2/1

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------  ----  -------------  -----  --------  ----------  ------------
 2/1      1     forwarding        19        32
enabled
```

Otra forma de visualizar la configuración de Portfast para un puerto, o más de uno, es ver la información del árbol de expansión para una VLAN determinada. Más adelante, en la sección de temporización de este documento, se muestra cómo hacer que el switch informe cada etapa del árbol de expansión por la que se mueve en tiempo real. Este resultado también muestra el tiempo de retraso de reenvío (15 segundos). Este es el tiempo que el spanning tree puede estar en el estado de escucha y el tiempo que puede estar en el estado de aprendizaje para cada puerto en la VLAN.

```
Switch-A (enable) show spantree 1
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-e0-4f-94-b5-00
Designated Root Priority    8189
Designated Root Cost        19
Designated Root Port        2/24
Root Max Age   20 sec    Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-90-92-b0-84-00
Bridge ID Priority          32768
Bridge Max Age 20 sec    Hello Time 2  sec   Forward Delay 15 sec

Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-Method
--------- ----  -------------  -----  --------  ----------  ------------

 2/1      1     forwarding        19        32   enabled
...
```

Para verificar que PAgP está apagado, utilice el comando **show port** channel. Especifique con certeza el número de módulo (2 en este caso) de modo que el comando muestre el modo del

canal aún si no se formó un canal. Si usted hace **show port** channel sin canales formados, simplemente dice no ports channeling. Usted quiere ir más allá y ver el modo de canal actual.

```
Switch-A (enable) show port channel
No ports channeling

Switch-A (enable) show port channel 2
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  notconnect auto      not channel
 2/2  notconnect auto      not channel
...
Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.

Switch-A (enable) show port channel 2
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  off       not channel
 2/2  connected  off       not channel
...
```

Para verificar que la negociación de trunking está desactivada, utilice el comando **set trunk** off. Usted muestra el estado predeterminado . A continuación, desactive el enlace troncal y muestre el resultado. Especifique el número de módulo 2 para que pueda ver el modo de canal actual para los puertos en este módulo.

```
Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         negotiate      not-trunking  1
 2/2      auto         negotiate      not-trunking  1
...

Switch-A (enable) set trunk 2/1-2 off
Port(s) 2/1-2 trunk mode set to off.

Switch-A (enable) show trunk 2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      off          negotiate      not-trunking  1
 2/2      off          negotiate      not-trunking  1
```

No es necesario, excepto en los casos más raros, desactivar la negociación automática de velocidad/dúplex o ajustar manualmente la velocidad y el dúplex en el switch. Si cree que es necesario para su situación, puede dar un ejemplo de cómo hacerlo en las Pruebas de sincronización con y sin DTP, PAgP y Portfast en una sección de Catalyst 5000.

Pruebas de sincronización con y sin DTP, PagP y PortFast en Catalyst 5000

Esta prueba muestra qué ocurre con la sincronización de la inicialización del puerto del switch mientras se ejecutan los distintos comandos. Las configuraciones predetermidas del puerto se usan en primer lugar para dar una referencia. PortFfast está desactivado, el modo PAgP (EtherChannel) está configurado como automático (canalizará si se lo pide) y el modo de concentración de enlaces (DTP) está configurado en automático (creará enlaces troncales si se lo

pide). La prueba luego activa PortFast y mide el tiempo, desactiva el PAgP y mide el tiempo, y desactiva el enlace troncal y mide el tiempo. Por último, se desactiva la negociación automática y se mide el tiempo. Todas estas pruebas se llevarán a cabo en Catalyst 5000 con una tarjeta Fast Ethernet 10/100 que admite DTP y PAgP.

Nota: Cuando el portfast está encendido, no es lo mismo que apagar el spanning tree (como se indica en el documento). Con portfast activado, el spanning tree aún se ejecuta en el puerto; simplemente no bloquea, escucha o aprende, y pasa inmediatamente al estado de reenvío. No se recomienda desactivar el árbol de expansión porque esto afecta toda la VLAN y puede hacer que la red sea vulnerable a los bucles de topología físicos, lo que puede causar serios problemas en la red.

Mostrar la versión y la configuración del IOS de Cisco del switch (**show version, show module**).

```
Switch-A (enable) show version
WS-C5505 Software, Version McpSW: 4.5(1) NmpSW: 4.5(1)
Copyright (c) 1995-1999 by Cisco Systems
NMP S/W compiled on Mar 29 1999, 16:09:01
MCP S/W compiled on Mar 29 1999, 16:06:50

System Bootstrap Version: 3.1.2

Hardware Version: 1.0  Model: WS-C5505  Serial #: 066507453

Mod Port Model      Serial #  Versions
--- ---- ---------- --------- -----------------------------------------
1   0    WS-X5530   006841805 Hw : 1.3
                               Fw : 3.1.2

                               Fw1: 3.1(2)
                               Sw : 4.5(1)
2   24   WS-X5225R  012785227 Hw : 3.2
                               Fw : 4.3(1)
                               Sw : 4.5(1)

       DRAM                    FLASH                   NVRAM
Module Total   Used    Free    Total   Used    Free    Total Used  Free
------ ------- ------- ------- ------- ------- ------- ----- ----- -----
1       32640K  13648K  18992K   8192K   4118K   4074K  512K  119K  393K

Uptime is 28 days, 18 hours, 54 minutes

Switch-A (enable) show module
Mod Module-Name         Ports Module-Type           Model    Serial-Num Status
--- ------------------- ----- --------------------- -------- --------- -------
1                       0     Supervisor III        WS-X5530  006841805 ok
2                       24    10/100BaseTX Ethernet WS-X5225R 012785227 ok
```

```
Mod MAC-Address(es)                         Hw     Fw         Sw
--- --------------------------------------- ------ ---------- -----------------
1   00-90-92-b0-84-00 to 00-90-92-b0-87-ff 1.3    3.1.2      4.5(1)
2   00-50-0f-b2-e2-60 to 00-50-0f-b2-e2-77 3.2    4.3(1)     4.5(1)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
--- -------- --------- ---------- ------
1   NFFC     WS-F5521  0008728786 1.0
```

Establezca el registro para el árbol de expansión en el modo más verboso (set logging level spantree 7). Este es el nivel de registro (2) predeterminado del árbol de expansión, lo que significa que se informarán solo las situaciones críticas.

```
Switch-A (enable) show logging

Logging buffer size:          500
        timestamp option:     enabled
Logging history size:         1
Logging console:              enabled
Logging server:               disabled
        server facility:      LOCAL7
        server severity:      warnings(4)

Facility            Default Severity         Current Session Severity
-------------       -----------------------  -----------------------
...
spantree            2                         2
...
0(emergencies)        1(alerts)             2(critical)
3(errors)             4(warnings)           5(notifications)
6(information)        7(debugging)
```

El nivel del árbol de expansión se cambia a 7 (debug), por lo que puede ver el cambio de estado del árbol de expansión en el puerto. Este cambio de configuración sólo dura para la sesión terminal, luego vuelve a la normalidad.

```
Switch-A (enable) set logging level spantree 7
System logging facility <spantree for this session set to severity 7(debugging)

Switch-A (enable) show logging
...

Facility            Default Severity         Current Session Severity
-------------       -----------------------  -----------------------
...
```

```
spantree            2                       7
...
```

Comenzar con el puerto ubicado en el cierre del Catalyst.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.
```

Ahora el tiempo y habilite el puerto. Usted quiere ver cuánto tiempo permanece en cada estado.

```
Switch-A (enable) show time
Fri Feb 25 2000, 12:20:17
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 12:20:39 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2000 Feb 25 12:20:39 %SPANTREE-6-PORTBLK: port 2/1 state in vlan 1 changed to blocking.
2000 Feb 25 12:20:39 %SPANTREE-6-PORTLISTEN: port 2/1 state in vlane 1 changed to Listening
.
2000 Feb 25 12:20:53 %SPANTREE-6-PORTLEARN: port 2/1 state in vlan 1 changed to Learning.
2000 Feb 25 12:21:08 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding.
```

Observe en el resultado que al puerto le llevó unos 22 segundos (20:17 a 20:39) comenzar la etapa de bloqueo del árbol de expansión. Este tiempo se destinó a negociar el enlace y realizar las tareas de DTP y PAgP. Cuando comience el bloqueo, estará ahora en el dominio del árbol de extensión. Desde el bloqueo del puerto, inmediatamente se escucha (20:39 a 20:39). El paso desde escuchar a aprender insumió aproximadamente 14 segundos (20:39 a 20:53).

Desde aprendizaje a reenvío tardó 15 segundos (de 20:53 a 21:08). Por lo tanto, el tiempo total antes de que el puerto entre en actividad para el tráfico, fue de aproximadamente 51 segundos (de 20:17 a 21:08).

Nota: Técnicamente, la etapa de escucha y aprendizaje es de 15 segundos, que es la forma en que se establece el parámetro de demora de reenvío para esta VLAN. La etapa de aprendizaje probablemente está más cerca de 15 segundos que de 14 segundos si se tienen mediciones más precisas. Ninguna de las mediciones aquí son perfectamente precisas. simplemente trataste de dar una idea de cuánto tardan las cosas.

Usted sabe por la salida y por el comando **show spantreecommand** que el spanning tree está activo en este puerto. Analicemos otros motivos que podrían retrasar al puerto en el alcance del estado de reenvío. **El comando show port** capabilities muestra que este puerto tiene la capacidad de conectarse mediante trunk y crear un EtherChannel. **El comando show** trunk indica que este puerto está en modo automático y que está configurado para negociar el tipo de trunking a utilizar (ISL o 802.1q, negociado a través del protocolo de trunking dinámico (DTP)).

```
Switch-A (enable) show port capabilities 2/1
Model                   WS-X5225R
Port                    2/1
Type                    10/100BaseTX

Speed                   auto,10,100
Duplex                  half,full
Trunk encap type        802.1Q,ISL
Trunk mode              on,off,desirable,auto,nonegotiate
Channel                 2/1-2,2/1-4
Broadcast suppression   percentage(0-100)
Flow control            receive-(off,on),send-(off,on)
Security                yes
Membership              static,dynamic
Fast start              yes
Rewrite                 yes
Switch-A (enable) show trunk 2/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      auto         negotiate      not-trunking  1
```

En primer lugar, puede habilitar Portfast en el puerto. La negociación de enlaces troncales (DTP) y EtherChannel (PAgP) aún se encuentra en modo automático.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.

Switch-A (enable) set spantree portfast 2/1 enable

Warning: Spantree port fast start should only be enabled on ports connected
to a single host.  Connecting hubs, concentrators, switches, bridges, and so on to
a fast start port can cause temporary spanning tree loops.  Use with caution.

Spantree port 2/1 fast start enabled.

Switch-A (enable) show time
Fri Feb 25 2000, 13:45:23
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
Switch-A (enable)
2000 Feb 25 13:45:43 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 13:45:44 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 change to forwarding.
```

Ahora dispone de un tiempo total de**21 segundos.**Tarda 20 segundos en unirse al grupo de puentes (de 45:23 a 45:43). Pero después, una vez habilitado Portfast, STP comienza a

reenviar en sólo un segundo (en lugar de 30 segundos). Ahorró 29 segundos al habilitar Portfast. Compruebe si puede reducir aún más el retraso.

Ahora usted pone el modo PAgP en "apagado". puede ver en el comando show port channel que el modo PAgP está configurado en *auto*, lo que significa que canaliza si un vecino que habla PAgP lo solicita. Debe desactivar los canales para al menos un grupo de dos puertos. No puede hacerlo para un solo puerto.

```
Switch-A (enable) show port channel 2/1
Port  Status     Channel   Channel     Neighbor                  Neighbor
                 mode      status      device                    port
----- ---------- --------- ----------- ------------------------- ----------
 2/1  connected  auto      not channel

Switch-A (enable) set port channel 2/1-2 off
Port(s) 2/1-2 channel mode set to off.
```

Apague el puerto y repita la prueba.

```
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.

Switch-A (enable) show time
Fri Feb 25 2000, 13:56:23
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 13:56:32 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 13:56:32 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to forwarding.
```

Observe que ahora solo toma 9 segundos alcanzar el estado de reenvío (56:23 a 56:32) en lugar de 21 segundos como en la prueba anterior. Al cambiar PAgP de autotooffin esta prueba ahorró aproximadamente 12 segundos.

Desactivemos el modo de enlace troncal (en vez de dejarlo en automático) y veamos cómo afecta al tiempo que le lleva al puerto alcanzar el estado de reenvío. De nuevo, apaga y enciende el puerto y graba el tiempo.

```
Switch-A (enable) set trunk 2/1 off
Port(s) 2/1 trunk mode set to off.
Switch-A (enable) set port disable 2/1
Port 2/1 disabled.
```

Iniciar la prueba con el troncal desactivado (en lugar de auto).

```
Switch-A (enable) show time
Fri Feb 25 2000, 14:00:19
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 14:00:22 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2000 Feb 25 14:00:23 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 change for forwarding.
```

ahorró unos segundos al principio, ya que solo tardó4 segundos en alcanzar el estado de reenvío del árbol de extensión (de 00:19 a 00:22). Ahorró unos 5 segundos al cambiar el modo de enlace troncal *deautotooff*.

(Opcional) Si el tiempo de inicialización del puerto del switch fue el problema, ya debe resolverse. Si tiene que afeitarse unos segundos más del tiempo, puede configurar el puerto manualmente la velocidad y el dúplex y no utilizar la negociación automática.

Si establece la velocidad y el dúplex manualmente en este lado, también debe establecer la velocidad y el dúplex en el otro lado. Esto se debe a que al establecer la velocidad y el dúplex del puerto se inhabilita la negociación automática en el puerto, y el dispositivo que se conecta no ve los parámetros de negociación automática. El dispositivo de conexión se conectará solo como semidúplex y la discordancia del dúplex resultante ocasionará un rendimiento inferior y errores en los puertos. Recuerde que si configura la velocidad y el dúplex de un lado, debe hacer lo mismo en el dispositivo de conexión para evitar estos problemas.

Para ver el estado del puerto después de establecer la velocidad y el puerto doshow dúplex.

```
Switch-A (enable) set port speed 2/1 100
Port(s) 2/1 speed set to 100Mbps.
Switch-A (enable) set port duplex 2/1 full
Port(s) 2/1 set to full-duplex.
Switch-A (enable) show port
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 2/1                     connected  1          normal   full   100 10/100BaseTX
...
```

Los resultados de sincronización son los siguientes:

```
Switch-A (enable) show time
Fri Feb 25 2000, 140528 Eastern
Switch-A (enable) set port enable 2/1
Port 2/1 enabled.
Switch-A (enable)
2000 Feb 25 140529 Eastern -0500 %PAGP-5-PORTTOSTP:Port 2/1 joined bridgeport 2/1
2000 Feb 25 140530 Eastern -0500 %SPANTREE-6-PORTFWD: port 2/1 state in vlan 1 changed to
```

forwarding.

El resultado final da un tiempo de **2 segundos**(0528 a 0530).

Realizó otra prueba temporizada visualmente iniciando un ping continuo (ping -t) dirigido al switch de un PC conectado al switch. A continuación, desconectó el cable del switch. Los pings comenzaron a fallar. Luego volvió a conectar el cable al switch y verificó estos relojes para ver cuánto tardaba el switch en responder a los pings desde el PC. Tomó alrededor de 5-6 segundos con la negociación automática para velocidad y dúplex encendidos y alrededor de 4 segundos con la negociación automática para velocidad y dúplex apagados.

Hay muchas variables en esta prueba (inicialización de PC, software de PC, respuestas del puerto de la consola del switch a las solicitudes, etc.), pero solo quería saber cuánto tiempo tardaría en obtener una respuesta desde el punto de vista de las PC. Todas las pruebas fueron desde el punto de vista del mensaje de depuración interno de los switches.

Cómo reducir el retardo de inicialización en el switch Catalyst 2900XL/3500XL

Los modelos 2900XL y 3500XL se pueden configurar desde un navegador web, mediante el SNMP o mediante la interfaz de línea de comandos (CLI). utilice la CLI. Este es un ejemplo donde puede ver el estado del spanning tree de un puerto, activar portfast y luego verificar que esté activado. El 2900XL/3500XL admite EtherChannel y trunking, pero no admite la creación dinámica de EtherChannel (PAgP) o la negociación dinámica de trunk (DTP) en la versión que ha probado (11.2(8.2)SA6), por lo que no tiene necesidad de desactivarlas en esta prueba. Además, después de activar portfast, el tiempo transcurrido para que el puerto se active ya es menos de 1 segundo, por lo que no tiene mucho sentido intentar cambiar la configuración de la negociación de velocidad/dúplex para acelerar las cosas. ¡espera que un segundo sea lo suficientemente rápido! PortFast está desactivado de forma predeterminada en los puertos del switch. Estos son los comandos para activar PortFast:

Configuración

```
2900XL#conf t
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#spanning-tree portfast
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#copy run start
```

Esta plataforma es como el router Cisco IOS; debe guardar la configuración (**copy run start**) si desea que se guarde permanentemente.

Verificación

Para verificar que PortFast esté habilitado, ejecute este comando:

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
```

```
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 2105, received 1
   The port is in the portfast mode
```

Observe la configuración del switch.

```
2900XL#show running-config
Building configuration...

Current configuration:
!
version 11.2
...
!
interface VLAN1
 ip address 172.16.84.5 255.255.255.0
 no ip route-cache
!
interface FastEthernet0/1
 spanning-tree portfast
!
interface FastEthernet0/2
!
...
```

Pruebas de Timing en el Catalyst 2900XL

Estas son las pruebas de sincronización en Catalyst 2900XL.

> La versión 11.2(8.2)SA6 del software se utilizó en 2900XL para estas pruebas.

```
Switch#show version
Cisco Internetwork Operating System Software
Cisco IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 11.2(8.2)SA6, MAINTENANCE
INTERIM SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 23-Jun-99 16:25 by boba
Image text-base: 0x00003000, data-base: 0x00259AEC

ROM: Bootstrap program is C2900XL boot loader

Switch uptime is 1 week, 4 days, 22 hours, 5 minutes
System restarted by power-on
System image file is "flash:c2900XL-c3h2s-mz-112.8.2-SA6.bin", booted via console

cisco WS-C2924-XL (PowerPC403GA) processor (revision 0x11) with 8192K/1024K bytes of
memory.
Processor board ID 0x0E, with hardware revision 0x01
Last reset from power-on

Processor is running Enterprise Edition Software
```

```
Cluster command switch capable
Cluster member switch capable
24 Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:50:80:39:EC:40
Motherboard assembly number: 73-3382-04
Power supply part number: 34-0834-01
Motherboard serial number: FAA02499G7X
Model number: WS-C2924-XL-EN
System serial number: FAA0250U03P
Configuration register is 0xF
```

desea que el switch nos diga qué sucede y cuándo sucede, por lo que debe ingresar estos comandos:

```
2900XL(config)#service timestamps debug uptime
2900XL(config)#service timestamps log uptime
2900XL#debug spantree events
Spanning Tree event debugging is on
2900XL#show debug
General spanning tree:
  Spanning Tree event debugging is on
```

Luego, apaga el puerto en cuestión.

```
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#shut
2900XL(config-if)#
00:31:28: ST: sent Topology Change Notice on FastEthernet0/6
00:31:28: ST: FastEthernet0/1 - blocking
00:31:28: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
down
00:31:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#
```

En este punto usted pega estos comandos del portapapeles en el switch. Estos comandos muestran el tiempo en el 2900XL y reactiva el puerto:

```
show clock
conf t
int f0/1
no shut
```

Por defecto, Portfast está desactivado. Puede confirmarlo de dos formas. La primera forma es que el comando **show spanning-tree** interface no mencione Portfast. La segunda manera es mirar esta configuración que se ejecuta y donde no se ve el comando **spanning-tree portfast** en la interfaz.

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 887, received 1
[Note: there is no message about being in portfast mode is in this spot...]

2900XL#show running-config
Building configuration...
...
!
interface FastEthernet0/1
[Note: there is no spanning-tree portfast command under this interface...]
!
```

Aquí está la primera prueba de temporización con Portfast desconectado.

```
2900XL#show clock
*00:27:27.632 UTC Mon Mar 1 1993
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#int f0/1
2900XL(config-if)#no shut
2900XL(config-if)#
00:27:27: ST: FastEthernet0/1 - listening
00:27:27: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:27:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
00:27:42: ST: FastEthernet0/1 - learning
00:27:57: ST: sent Topology Change Notice on FastEthernet0/6
00:27:57: ST: FastEthernet0/1 - forwarding
```

El tiempo total desde el apagado hasta que el puerto inició el reenvío fue de **30 segundos** (de 27:27 a 27:57)

Para activar PortFast, haga lo siguiente:

```
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#interface fastEthernet 0/1
2900XL(config-if)#spanning-tree portfast
2900XL(config-if)#exit
2900XL(config)#exit
2900XL#
```

Para verificar que Portfast está habilitado, utilice el comando **show spanning-tree** interface. Observe que el resultado del comando (casi al final) indica que Portfast está habilitado.

```
2900XL#show spanning-tree interface fastEthernet 0/1
Interface Fa0/1 (port 13) in Spanning tree 1 is FORWARDING
   Port path cost 19, Port priority 128
   Designated root has priority 8192, address 0010.0db1.7800
   Designated bridge has priority 32768, address 0050.8039.ec40
   Designated port is 13, path cost 19
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 1001, received 1

The port is in the portfast mode
```

También puede observar que Portfast se activa en la salida de configuración.

```
2900XL#sh  ru
Building configuration...
...
interface FastEthernet0/1
 spanning-tree portfast

...
```

Ahora hagamos la prueba de sincronización con PortFast habilitado.

```
2900XL#show clock
*00:23:45.139 UTC Mon Mar 1 1993
```

```
2900XL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
2900XL(config)#int f0/1
2900XL(config-if)#no shut
2900XL(config-if)#
00:23:45: ST: FastEthernet0/1 -jump to forwarding from blocking
00:23:45: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:23:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

En este caso, el tiempo total fue inferior a **1 segundo**. Si el problema fue la demora de inicialización del puerto en el switch, portfast debe resolverlo.

Recuerde que el switch no admite actualmente la negociación de trunk, por lo que no necesita desactivarlo. Tampoco admite PAgP para trunking, por lo que tampoco es necesario desactivarlo. El switch admite la negociación automática de velocidad y dúplex, pero dado que el retraso es tan pequeño, esto no sería una razón para desactivarlo.

también realizó la prueba de ping desde una estación de trabajo al switch. La respuesta del switch tardó aproximadamente 5-6 segundos en llegar, independientemente de si la negociación automática de velocidad y dúplex estaba activada o desactivada.

Cómo reducir el retardo de inicialización en el switch Catalyst 1900/2800

Los 1900/2820 se refieren a Portfast con otro nombre: Spantree Start-Forwarding. Para la versión de software, que ejecuta (V8.01.05), los switches tienen de forma predeterminada el siguiente valor: Portfast está activado en los puertos Ethernet (10 Mbps) y Portfast está desactivado en los puertos Fast Ethernet (uplink). Por lo tanto, cuando **usted muestra** runto para ver la configuración, si un puerto Ethernet no dice nada sobre Portfast, entonces Portfast está habilitado. Si dice "no spantree start-forwarding" en la configuración, PortFast está deshabilitado. En un puerto FastEthernet (100 Mbps), ocurre lo contrario: para un puerto FastEthernet, Portfast está activado sólo si el puerto muestra "spantree start-forwarding" en la configuración.

Aquí hay un ejemplo de cómo configurar Portfast en un puerto FastEthernet. Estos ejemplos utilizan la versión 8 de Enterprise edition software (Software de edición para empresas). 1900 guarda automáticamente la configuración después de que se hayan realizado los cambios. Recuerde que no desea que PortFast esté habilitado en ningún puerto que se conecta a otro switch o concentrador; solo cuando el puerto se anexa a una estación final. La configuración se guarda automáticamente en NVRAM.

Configuración

```
1900#show version
Cisco Catalyst 1900/2820 Enterprise Edition Software
Version V8.01.05
Copyright (c) Cisco Systems, Inc.  1993-1998
1900 uptime is 0day(s) 01hour(s) 10minute(s) 42second(s)
cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory
Hardware board revision is 5
```

```
Upgrade Status: No upgrade currently in progress.
Config File Status: No configuration upload/download is in progress
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-50-50-E1-A4-80
1900#conf t
Enter configuration commands, one per line.  End with CNTL/Z
1900(config)#interface FastEthernet 0/26
1900(config-if)#spantree start-forwarding
1900(config-if)#exit
1900(config)#exit
1900#
```

Verificación

Una forma de verificar si PortFast está activado es consultando la configuración. Recuerde que un puerto FastEthernet debe decir que está prendido. La tiene un puerto Ethernet salvo que la configuración muestre que está desactivada. En esta configuración, la interfaz Ethernet 0/1 tiene PortFast desactivado (puede ver el comando para desactivarlo), la interfaz Ethernet 0/2 tiene PortFast activado (no se ve nada, lo que significa que está activado) y la interfaz FastEthernet 0/26 (puerto A en el sistema de menú) tiene PortFast activado (puede visualizar el comando para activarlo).

```
1900#show running-config
Building configuration...
...
!
interface Ethernet 0/1

  no spantree start-forwarding
!
interface Ethernet 0/2

!
...
!
interface FastEthernet 0/26
  spantree start-forwarding
```

La forma más sencilla de visualizar el estado portfast es a través del sistema de menú. Si elige (**P**) para Port Configuration en el menú principal y luego elige **port**, la salida indica si el modo Port Fast está habilitado. Este resultado corresponde al puerto FastEthernet 0/26, que es el puerto "A" en este switch.

```
        Catalyst 1900 - Port A Configuration

        Built-in 100Base-FX
        802.1d STP State:  Blocking     Forward Transitions:  0

    ---------------------- Settings ----------------------------------------
     [D] Description/name of port
     [S] Status of port                              Suspended-no-linkbeat
     [I] Port priority (spanning tree)               128 (80 hex)
     [C] Path cost (spanning tree)                   10
     [H] Port fast mode (spanning tree)              Enabled
     [E] Enhanced congestion control                 Disabled
     [F] Full duplex / Flow control                  Half-Duplex
```

```
    ---------------------- Related Menus ----------------------------------
     [A] Port addressing           [V] View port statistics
     [N] Next port                 [G] Goto port
     [P] Previous port             [X] Exit to Main Menu

Enter Selection:
```

Pruebas de sincronización en el Catalyst 1900

Los valores de sincronización son más difíciles de verificar en un 1900/2820 debido a la falta de herramientas de depuración, por lo que acaba de iniciar un ping desde una PC conectada al switch dirigido al propio switch. desconectó y luego volvió a conectar el cable y registró cuánto tiempo le tomó al switch responder al ping con Portfast activado y con Portfast desactivado. Para un puerto Ethernet con Portfast activado (el estado predeterminado), el PC recibió una respuesta en un plazo de **5-6 segundos**. Con Portfast apagado la PC recibió una respuesta en 34 a 35 segundos.

Beneficio adicional de Portfast

Hay otro beneficio relacionado con el árbol de expansión para utilizar PortFast en su red. Cada vez que se active un enlace y se mueva al estado de reenvío en el árbol de expansión, el switch enviará un paquete de árbol de expansión especial llamado notificación de cambio de topología (TCN). La TCN pasa a la raíz del árbol de expansión, donde se propaga a todos los switches de la VLAN. Esto hace que todos los switches desactualicen sus tablas de direcciones MAC con el parámetro de retardo de reenvío. El parámetro de retardo de reenvío normalmente está configurado en 15 segundos. Cada vez que una estación de trabajo se une al grupo de puentes, las direcciones MAC de todos los switches quedan sin vigencia en 15 segundos en lugar de hacerlo en 300 segundos, como es habitual.

Dado que cuando una estación de trabajo entra en actividad, en realidad no cambia la topología en ninguna medida importante, en lo que respecta a todos los switches en la VLAN, no es necesario que atraviesen el período TCN de rápido vencimiento. Si enciende PortFast, el switch no enviará paquetes TCN cuando se active el puerto.

Comandos que se deben utilizar para verificar que la configuración funciona

Esta es una lista de los comandos que se deben usar para verificar si la configuración funciona.

4000/5000/6000

show port spantree 2/1; vea si la característica "Fast-Start" (Portfast) está activada o desactivada

show spantree 1- vea todos los puertos en VLAN 1 y si tienen habilitado "Fast-Start"

show port channel – vea si tiene algunos canales activos

show port channel 2: consulte el modo de canal (automático, apagado, etc.) para cada puerto del módulo 2

show trunk 2- vea el modo trunk (auto, off, etc.) para cada puerto en el módulo 2

show port - muestra el estado (conectado, no conectado, etcétera), la velocidad, el dúplex para todos los puertos en el switch

2900XL/3500XL

show spanning-tree interface FastEthernet 0/1 – para ver si Portfast está habilitado en este puerto (si Portfast no se menciona es que no está habilitado)

show running-config - si un puerto muestra el comando spanning-tree portfast, la función Portfast está habilitada.

1900/2800

show running-config - para ver las configuraciones actuales (algunos comandos son invisibles cuando representan los valores predeterminados de la configuración del switch)

Utilice el sistema de menú para la pantalla de estado del puerto.

Comandos para usar para la resolución de problemas de configuración

Esta es una lista de comandos para usar para la resolución de problemas de configuración.

4000/5000/6000

show port spantree 2/1; vea si la característica "Fast-Start" (Portfast) está activada o desactivada

show spantree 1- vea todos los puertos en VLAN 1 y si tienen habilitado "Fast-Start"

show port channel – vea si tiene algunos canales activos

show port channel 2: consulte el modo de canal (automático, apagado, etc.) para cada puerto del módulo 2

show trunk 2- vea el modo trunk (auto, off, etc.) para cada puerto en el módulo 2

show port - muestra el estado (conectado, no conectado, etc.), la velocidad, el dúplex para todos los puertos en el switch

show logging: observa qué tipo de mensajes genera el resultado del registro.

set logging level spantree 7: establece el switch para registrar el puerto del árbol de expansión, indicando el tiempo real en la consola.

set port disable 2/1 – Desactive el puerto en software (como "apagado" en el router)

set port enable 2/1 - activa el puerto en el software (como “no shutdown" en el router)

show time: muestra el tiempo actual en segundos (que se usa al comienzo de una prueba de sincronización).

show port capabilities – vea que características se implementan en el puerto.

set trunk 2/1 off - establecer el modo de conexión troncal en off (para acelerar el tiempo de inicialización del puerto)

set port channel 2/1-2 off - establecer el modo EtherChannel (PAgP) en off (para acelerar el tiempo de inicialización del puerto)

set port speed 2/1 100- ajuste el puerto a 100Mbps y desactive la negociación automática

set port duplex 2/1 full: Establece el dúplex de puerto completo

2900XL/3500XL

service timestamps debug uptime - muestra la hora con los mensajes de depuración

service timestamps log uptime - muestra la hora con los mensajes del registro.

debug spantree events: muestra cuándo el puerto pasa por las etapas del árbol de expansión.

show clock - para ver el tiempo actual (para las pruebas de sincronización)

show spanning-tree interface FastEthernet 0/1 – para ver si Portfast está habilitado en este puerto (si Portfast no se menciona es que no está habilitado)

shut: activa un puerto desde el software.

no shut (no cierre) - para activar un puerto desde el software.

1900/2800

show running-config - para ver las configuraciones actuales (algunos comandos son invisibles cuando representan los valores predeterminados de la configuración del switch)

Configuración y resolución de problemas de IP Multilayer Switching (MLS)

Objetivos

Este documento describe cómo resolver problemas de Multilayer Switching (MLS) para IP. Esta característica se ha convertido en un método altamente deseado con el que acelerar el rendimiento del routing mediante el uso de circuitos integrados específicos de aplicaciones dedicadas (ASIC). El ruteo tradicional se realiza a través de una CPU central y un software; MLS descarga una porción significativa del ruteo (reescritura de paquetes) al hardware y también se le ha denominado switching. MLS y conmutación de tres capas son términos equivalentes. La función NetFlow de Cisco IOS es distinta y no se trata en este documento. MLS también incluye soporte para IPX (IPX MLS) y multidifusión (MPLS), pero este documento se centra exclusivamente en cómo resolver problemas de IP MLS básico.

Introducción

A medida que se formulan mayores demandas a las redes, mayor será la necesidad de mejor rendimiento. Cada vez se conectan más PC a la LAN, WAN e Internet y los usuarios requieren un acceso rápido a bases de datos, archivos/páginas web, aplicaciones de red, otras PC y videos de flujo continuo. Para que las conexiones se mantengan veloces y confiables, las redes deben poder ajustarse rápidamente a los cambios y las fallas y deben poder encontrar la mejor ruta, mientras se mantienen lo más invisible posible para los usuario finales. Los usuarios finales que experimentan un flujo de información rápido entre sus PC y el servidor con lentitud de red mínima son los más felices. La determinación de la mejor trayectoria es la función principal de los protocolos de ruteo, y esto puede ser un proceso intensivo de la CPU; se obtiene un aumento significativo del rendimiento al descargar una parte de esta función al hardware de switching. Este es el punto de la función de MLS.

Hay tres componentes principales de MLS: dos de ellos son MLS-RP y MLS-SE. El MLS-RP es el router de MLS que realiza la función tradicional de routing entre las subredes/VLAN. El MLS-SE es un switch habilitado para MLS que, generalmente, requiere un router para el ruteo entre subredes/VLAN, aunque con hardware y software especial puede encargarse de la reescritura del paquete. Cuando un paquete atraviesa una interfaz enrutada, las porciones sin datos del paquete se modifican (reescriben) mientras el paquete se transfiere a su destino, salto a salto. Aquí puede surgir confusión, ya que parece que un dispositivo de capa 2 asume una tarea de capa 3; en realidad, el switch solo está reescribiendo la información de capa 3 y está cambiando entre subredes/VLAN; el router sigue siendo responsable de los cálculos de ruta basados en estándares y de la determinación de la mejor ruta. Gran parte de esta confusión se puede evitar si mantiene mentalmente las funciones de routing y switching por separado, especialmente cuando, como suele ser el caso, se encuentran dentro del mismo chasis (como con un MLS-RP interno). Piense en MLS como una forma mucho más avanzada de almacenar en caché el router, con la caché separada del router en un switch. Tanto el MLS-RP como el MLS-SE, junto con los requisitos mínimos correspondientes de hardware y software, se requieren para MLS.

El MLS-RP puede ser interno (instalado en un chasis de switch) o externo (conectado a través de un cable a un puerto de enlace troncal en el switch). Ejemplos de MLS-RP internos son el Módulo de switch de ruta (RSM) y la Tarjeta de función de switch de ruta (RSFC), que se instalan en una

ranura o supervisor de un miembro de la familia Catalyst 5xxx, respectivamente; lo mismo se aplica a la Tarjeta de función de switch multicapa (MSFC) para la familia Catalyst 6xxx. Los ejemplos de MSL-RP externos incluyen cualquier miembro de los routers de las series Cisco 7500, 7200, 4700, 4500 o 3600. En general, para soportar la función MLS IP, todos los MLS-RP requieren una versión mínima del IOS de Cisco en los trenes 11.3WA o 12.0WA; consulte la documentación de la versión para más detalles. Además, **MLS debe estar** habilitado para que un router sea un MLS-RP.

El MLS-SE es un switch con hardware especial. Para un miembro de la familia Catalyst 5xxx, MLS requiere que el supervisor tenga instalada una tarjeta de función NetFlow (NFFC); Supervisor IIG e IIIG tienen una de forma predeterminada. Además, se requiere como mínimo el software Catalyst OS 4.1.1. Observe que la serie 4.x se ha convertido en la 'implementación general' (GD) o satisface los criterios rigurosos del usuario final y los objetivos de estabilidad según la experiencia en el campo; por lo tanto, revise el sitio web de Cisco para acceder a las últimas versiones. IP MLS se admite y habilita automáticamente el para software y hardware Catalyst 6xxx con MSFC/PFC (otros routers tienen el MLS desactivado en forma predeterminada) Tenga en cuenta que IPX MLS y MLS para multidifusión pueden tener diferentes requisitos de hardware y software (Cisco IOS y Catalyst OS). Más plataformas de Cisco admiten o pueden admitir la función MLS. Además, **MLS debe estar** habilitado para que un switch sea MLS-SE.

El tercer componente importante de MLS es el Protocolo de conmutación de capas múltiples (MLSP). Esto se debe a que cuando comprende los conceptos básicos de MLSP se encuentra en el corazón de MLS, y esto es esencial para resolver eficazmente los problemas de MLS. MLSP es utilizado por el MLS-RP y el MLS-SE para comunicarse entre sí; las tareas que habilitan el MLS y los flujos de instalación, actualización o eliminación (información de caché), y la administración y exportación de las estadísticas de flujo (NetFlow Data Export se cubre en otra documentación). MLSP también le permite a MLS-SE conocer las direcciones de Control de acceso de medios (MAC, capa 2) de las interfaces habilitadas para MLS, revisar la máscara de flujo del MLS-RP (explicado más adelante en este documento) y confirmar que el MLS-RP está operacional. El MLS-RP envía paquetes de 'saludo' de multidifusión cada 15 segundos con MLSP; si se pierden tres de estos intervalos, el MLS-SE reconoce que el MLS-RP ha fallado o que se ha perdido la conectividad con él.

El diagrama ilustra tres aspectos esenciales que se deben completar (con MLSP) para crear un acceso directo: los pasos de candidato, habilitador y almacenamiento en caché. El MLS-SE verifica una entrada MLS en caché; si la entrada de memoria caché MLS y la información del paquete coinciden (un acierto), el encabezado del paquete se reescribe localmente en el switch (un acceso directo o una derivación del router) en lugar de enviarse al router como suele suceder. Los paquetes que no coinciden y que se envían al MLS-RP son paquetes candidatos; es decir, existe la posibilidad de conmutarlos localmente. Luego de transmitir el paquete candidato a través de la máscara de flujo de MLS (que se explica en la próxima sección) y volver a escribir la información incluida en el encabezado del paquete (la parte de los datos no se toca), el router lo envía hacia el salto siguiente a través del trayecto de destino. El paquete se denomina ahora paquete facilitador. Si el paquete regresa al mismo MLS-SE desde el que salió, se crea un acceso directo MLS y se coloca en la memoria caché MLS; la reescritura para ese paquete y todos los paquetes similares que los rastrean (llamados flujo) ahora se realiza localmente por el hardware del switch en lugar de por el software del router. **El mismo MLS-SE debe ver los paquetes candidatos y habilitadores para un flujo particular para que se cree un acceso directo MLS** (esta es la razón por la que la topología de red es importante para MLS). Recuerde, el objetivo de la MLS es permitir el trayecto de comunicación entre dos dispositivos que se encuentran en diferentes VLAN, conectados fuera del mismo switch para eludir al router y mejorar el rendimiento de la red.

Mediante el uso de la máscara de flujo (esencialmente una lista de acceso), el administrador

puede ajustar el grado de similitud de estos paquetes y ajustar el alcance de los flujos: dirección de destino; direcciones de destino y origen; o información de destino, origen y capa cuatro. Tenga en cuenta que el primer paquete de un flujo siempre pasa a través del router; a partir de ese momento, se conmuta localmente. Cada flujo es unidireccional; la comunicación entre los PC, por ejemplo, requiere la configuración y el uso de dos accesos directos. El objetivo principal de MLSP es configurar, crear y mantener estos accesos directos.

Estos tres componentes (MLS-RP, MLS-SE y MLSP) liberan recursos vitales del router cuando permite que otros componentes de la red asuman algunas de sus funciones. En función de la topología y la configuración, MLS proporciona un método sencillo y muy eficaz que aumenta el rendimiento de la red en la LAN.

Resolución de problemas de tecnología IP MLS

Se incluye y se discute un diagrama de flujo para utilizar para resolver problemas de MLS IP básico. Se deriva de los tipos más comunes de casos de MLS-IP abiertos con el sitio web de soporte técnico de Cisco y a los que se enfrentaban los usuarios y los ingenieros de soporte técnico hasta el momento en que se creó este documento. MLS es una función robusta, y no debe tener problemas con ella; si surge un problema, esto le ayuda a resolver los tipos de problemas de MLS IP a los que probablemente se enfrente. Se hacen algunas suposiciones esenciales:

- Conoce los pasos de configuración básicos necesarios para habilitar IP MLS en el router y los switches y ha completado estos pasos: consulte los recursos enumerados al final de este documento para obtener material excelente.

- El IP Routing está habilitado en el MLS-RP (está activado de forma predeterminada): si el comando **command ip routing** aparece en la configuración global de **ashow run**, se ha desactivado y el IP MLS no funciona.

- Existe conectividad IP entre MLS-RP y MLS-SE:haga ping a las direcciones IP del router desde el switch y busque signos de exclamación (llamados "bangs") para que se muestren a cambio.

- Las interfaces MLS-RP se encuentran en estado 'up/up' en el router: **escriba show ip interface** brief en el router para confirmar esto.

Advertencia: Siempre que realice cambios de configuración en un router destinado a ser permanente, recuerde guardar esos cambios con **acopy running-config starting-config**(versiones abreviadas de este comando **includecopy run startandwr mem).** Las modificaciones de configuración se pierden si el router se vuelve a cargar o restablece. El RSM, la RSFC y la MSFC son routers, no switches. Por el contrario, los cambios que se realizaron en el indicador del switch de un miembro de la familia Catalyst 5xxx o 6xxx, se guardan automáticamente.

Esta sección soluciona problemas de tecnología de MLS IP.

- ¿Se cumplen los requisitos mínimos de software y hardware?

  Actualice el MLS-RP y SE para satisfacer los requisitos mínimos de software y hardware.

Para el MLS-RP, no se necesita ningún hardware adicional. Si bien se puede configurar la MLS en las interfaces no troncales, la conexión al MLS-SE se da generalmente a través de las interfaces de VLAN (como mediante un RSM) o admite enlaces troncales (se puede configurar para transportar información de VLAN mediante la configuración de ISL o 802.1q). Recuerde también que, a la fecha de publicación, solo los miembros de las familias 7500, 7200, 4700, 4500 y 3600 del router admiten la MLS de forma externa. Actualmente, solo estos routers externos y los routers que encajan con las familias de switches Catalyst 5xxx o 6xxx (como el RSM y la RSFC para la familia Catalyst 5xxx y la MSFC para la familia Catalyst 6xxx) pueden ser MLS-RP. MSFC también requiere la Tarjeta de características de políticas (PFC), ambas instaladas en Catalyst 6xx Supervisor. IP MLS es ahora una función estándar en Cisco IOS 12.0 y software de router posterior. El software Cisco IOS inferior a Cisco IOS 12.0 generalmente requiere un tren especial; para tal soporte de IP MLS, instale las imágenes más recientes en Cisco IOS 11.3 que tengan las letras 'WA' en sus nombres de archivo.

Para MLS-SE, se requiere una tarjeta de función NetFlow (NFFC) para un miembro de la familia Catalyst 5xxx; esta tarjeta se instala en el módulo Supervisor del switch Catalyst y se incluye como hardware estándar en los supervisores Catalyst 5xxx más nuevos (es decir, desde 1999). No se admite NFFC en los Supervisor I o II y es una opción para los primeros Supervisor III. Además, se necesita un mínimo de 4.1.1 CatOS para IP MLS. Por el contrario, para la familia Catalyst 6xxx, el hardware requerido viene como equipo estándar y MLS IP ha sido admitida desde la primera versión de software de CatOS 5.1.1 (de hecho, MLS IP es un ingrediente esencial y predeterminado por su alto rendimiento). Con las nuevas plataformas y software que admiten IP MLS, es importante revisar la documentación y las notas de la versión, y generalmente instalar la última versión en el tren más bajo que cumpla con sus requisitos de funciones. Verifique siempre las notas de la versión y consulte en la oficina de ventas local de Cisco para obtener nuevos desarrollos de características y soporte MLS.

Los comandos fusionados para verificar que la versión de **show** del hardware y el software instalados en el router **y el módulo show** en el switch

Nota: La familia de switches Catalyst 6xxx NO admite un MLS-RP externo en este momento. El MLS-RP debe ser una MSFC.

¿Los dispositivos de origen y destino en diferentes VLAN se encuentran en el mismo MLS-SE y comparten un solo MLS-RP común?

Es un requisito básico de topología de MLS que el router tenga un trayecto hacia cada una de las VLAN. Recuerde que el punto de MLS es crear un acceso directo entre dos VLAN, de modo que el ruteo entre los dos dispositivos extremos pueda ser realizado por el switch, y esto libere al router para otras tareas. En realidad, el switch no enruta; reescribe las tramas de modo que aparezca a los dispositivos finales que hablan a través del router. Si ambos dispositivos están conectados a la misma VLAN, el MLS-SE cambia la trama localmente sin utilizar la MLS del mismo modo que los switches en un entorno conectado con puentes de forma transparente; no se creará ningún acceso directo a la MLS. Uno puede tener routers y switches múltiples en la red, e incluso switches múltiples a lo largo del trayecto del flujo, pero el trayecto entre los dos dispositivos finales para los que uno desea tener un acceso directo de MLS debe incluir una sola MLS-RP para dicho trayecto. En otras palabras, el flujo desde la fuente al destino debe cruzar un límite de VLAN en la misma MLS-RP y un par de paquetes candidato y activador debe ser visto por el mismo MLS-SE para que se cree el acceso directo de MLS. Si no se cumple con estos criterios, entonces el paquete se enrutará normalmente sin el uso de la MLS. Consulte los documentos que se sugieren al final de este

documento para conocer los diagramas y los debates relacionados con las topologías de red admitidas y no admitidas.

¿El MLS-RP contiene la sentencia **anmls rp** bajo su configuración global y de interfaz?

Si uno no está presente, **addmls rp** ipstatement apropiadamente en el MLS-RP. Excepto para los routers cuyas IP MLS se habilitan automáticamente (como en los Catalyst 6xxx MSFC), este es un paso de configuración requerido. En la mayoría de los MLS-RP (routers configurados para IP MLS), este enunciado debe apareces tanto en la configuración global como en la configuración de la interfaz.

Nota: Cuando configure el MLS-RP, recuerde también colocar el comando **themls rp management-**interface bajo una de sus interfaces IP MLS. Este paso necesario indica al MLS-RP a qué interfaz debe enviar los mensajes del MLSP para comunicarse con el MLS-SE. Nuevamente, es necesario colocar este comando únicamente bajo una interfaz.

¿Hay alguna característica configurada en MLS-RP que desactive automáticamente MLS en la interfaz?

Existen varias opciones de configuración en el router que no son compatibles con la MLS. Éstas incluyen contabilidad de IP, encripción, compresión, seguridad IP, Traducción de direcciones de red (NAT) y Velocidad de acceso comprometida (CAR). Para obtener más información, consulte los enlaces sobre la configuración de la MLS IP incluidos al final de este documento. Los paquetes que atraviesan una interfaz de router configurada con cualquiera de estas funciones deben enrutarse con normalidad; no se crea ningún acceso directo MLS. Para que la MLS funcione, deshabilite estas funciones en la interfaz del MLS-RP.

Otra característica importante que afecta a MLS son las listas de acceso, las de entrada y salida. En 'Máscaras de flujo' se incluye un análisis adicional de esta opción.

¿El MLS-SE reconoce la dirección MLS-RP?

Para que MLS funciones, el switch debe reconocer al router como un MLS-RP. Los MLS-RP internos (una vez más, el RSM o RSFC en un miembro de la familia Catalyst 5xxx y el MSFC en un miembro de la familia Catalyst 6xxx) son reconocidos automáticamente por el MLS-SE en el que están instalados. Para los MLS-RP externos, uno debe informar explícitamente al switch de la dirección del router. Esta dirección no es realmente una dirección IP, aunque en MLS-RPs externos se elige de la lista de direcciones IP configuradas en las interfaces del router; es simplemente un ID de router. De hecho, para MLS-RPs internos, el MLS-ID normalmente ni siquiera es una dirección IP configurada en el router; dado que los MLS-RPs internos se incluyen automáticamente, normalmente es una dirección de loopback (127.0.0.x). Para que MLS funcione, incluya en MLS-SE el MLS-ID que se encuentra en MLS-RP.

Utiliza show mls rpon the router para encontrar el ID de MLS. Luego configure ese ID en el switch con el comando **set mls include <MLS-ID>**. Este paso de configuración es obligatorio cuando se utilizan MLS-RP externos.

Nota: Si cambia la dirección IP de las interfaces MLS-RP y luego recarga el router, puede hacer que el proceso MLS del router elija un nuevo ID MLS. Este nuevo MLS-ID puede ser diferente del MLS-ID que se incluyó manualmente en el MLS-SE, lo que puede hacer que

MLS se detenga; esto no es un error de software, sino un efecto del switch que intenta comunicarse con un MLS-ID que ya no es válido. Asegúrese de incluir esta nueva ID de MLS en el switch para que la MLS funcione una vez más. También puede que sea necesario deshabilitar/habilitar la MLS IP.

Nota: Cuando el MLS-SE no está conectado directamente al MLS-RP, como con esta topología, la dirección que debe incluirse en el MLS-SE puede aparecer como la dirección de loopback mencionada: un switch conectado entre el MLS-SE y el MLS-RP. Debe incluir MLS-ID aunque MLS-RP sea interno. Para el segundo switch, el MLS-RP aparece como un router externo, ya que el MLS-RP y el MLS-SE no están contenidos en el mismo chasis.

¿La interfaz de MLS-RP y el MLS-SE están en el mismo dominio VTP activado?

MLS requiere que los componentes de MLS, junto con las estaciones finales, estén en el mismo dominio de Virtual Trunking Protocol (VTP). El VTP es un protocolo de capa dos que se utiliza para administrar las VLAN en varios switches Catalyst desde un switch central. Permite a un administrador crear o eliminar una VLAN en todos los switches de un dominio y no tiene que hacerlo en todos los switches de ese dominio. El protocolo de conmutación multicapa (MLSP), que MLS-SE y MLS-RP utilizan para comunicarse entre sí, no cruza un límite de dominio VTP. Si el administrador de red tiene VTP habilitado en los switches (VTP está habilitado en los miembros de la familia Catalyst 5xxx y 6xxx de forma predeterminada), utilice el comando **show vtp domainen el switch para saber en qué dominio VTP se ha ubicado el MLS-SE.** Excepto para el Catalyst 6xxx MSFC, en el que MLS es esencialmente *una función plug-and-*play, a continuación debe agregar el dominio VTP a cada una de las interfaces MLS del router. Esto permite que las multidifusiones del MLSP se muevan entre el MLS-RP y el MLS-SE; por lo tanto, permiten que la MLS funcione.

En el modo de configuración de interfaz del MLS-RP, introduzca los siguientes comandos:

no mls rp ipDisable MLS en la interfaz MLS-RP afectada antes de modificar el dominio VTP.

mls rp vtp-domain< VTP domain name> : el nombre de dominio del VTP en cada interfaz habilitada para la MLS debe coincidir con el del switch.

mls rp vlan-id<VLAN #> : solo se requiere para los enlaces troncales que no son ISL y las interfaces del MLS-RP externo.

mls rp management-interfaceRealice esto para una sola interfaz en el MLS-RP. Este paso requerido indica al MLS-RP desde qué interfaz debe enviar mensajes MLSP.

mls rp ipEnable MLS una vez más en la interfaz de MLS-RP.

Para cambiar el nombre de dominio del VTP del MLS-SE, utilice este comando en el mensaje de activación de CatOS del switch:

set vtp domain name <nombre de dominio VTP>

Para que MLS funcione, asegúrese de que VTP esté habilitado en el switch:

set vtp enable

¿Las máscaras de flujo coinciden sobre MLS-RP y MLS-SE?

Una máscara de flujo es un filtro configurado por un administrador de red que MLS utiliza

para determinar si es necesario crear un acceso directo. Al igual que una lista de acceso, cuanto más detallados sean los criterios que configure, más profundo será el proceso de MLS para verificar si el paquete cumple con esos criterios. Para ajustar el alcance de los accesos directos creados por MLS, la máscara de flujo se puede hacer más o menos específica; la máscara de flujo es esencialmente un dispositivo de sintonía. Existen tres tipos de modos IP MLS: IP de destino, IP de origen de destino e IP de flujo completo. El modo IP de destino (valor predeterminado) se usa cuando no se aplica ninguna lista de acceso a la interfaz de MLS habilitada del router. El modo IP de origen y destino se usa cuando se aplica una lista de acceso estándar. La IP de flujo completo es de hecho para una lista de acceso ampliado. El modo MLS en el MLS-RP está implícitamente determinado por el tipo de lista de acceso aplicado a la interfaz. Por el contrario, el modo MLS del MLS-SE está explícitamente configurado. Si selecciona el modo adecuado, el usuario puede configurar la MLS de manera que solo coincida la dirección de destino para crear un acceso directo de la MLS o tanto del origen como el destino e incluso la información de capa cuatro, como los números de los puertos TCP/UDP.

El modo MLS es configurable tanto con el MLS-RP como con el MLS-SE y, en general, deben coincidir. Si se considera que se requieren los modos IP de origen-destino o MLS IP de flujo completo, es mejor configurarlo en el router y aplicar la lista de acceso adecuada. La MLS siempre elige la máscara más específica. Le da a la máscara de flujo configurada en el MLS-RP precedencia sobre la que se encuentra en el MLS-SE. TENGA CUIDADO si cambia el modo MLS del switch desde el ip de destino predeterminado: debe asegurarse de que coincida con el modo MLS en el router para que MLS funcione. Para los modos source-destination-ip y full-flow-ip, recuerde aplicar la lista de acceso a la interfaz de router apropiada; sin lista de acceso aplicada, incluso si está configurada, el modo MLS simplemente es destination-ip, el predeterminado.

Advertencia: Siempre que se cambia la máscara de flujo, ya sea en MLS-RP o MLS-SE, se depuran todos los flujos MLS almacenados en caché y se reinicia el proceso MLS. Una purga también puede ocurrir cuando aplica el comando **clear ip route-cache** en el router. Si aplica el **comando de** configuración global del router **ip routing**, que desactiva el ruteo IP y básicamente transforma el router en un puente transparente, causa una purga y deshabilita MLS (recuerde que el ruteo es un requisito previo de MLS). Cada uno de estos puede afectar temporalmente, pero de forma grave, el rendimiento del router en una red de producción. El router experimentará un pico en su carga hasta que se creen los nuevos accesos directos, ya que ahora debe administrar todos los flujos anteriormente procesados a través del switch.

Nota: Especialmente con un miembro de la familia Catalyst 5000 como MLS-SE, debe evitar el uso muy amplio de máscaras de flujo configuradas con información de capa cuatro. Si se fuerza el router para entablar relaciones de par tan profundamente con cada paquete en la interfaz, se pierden muchos de los beneficios propios de la MLS. Esto no es un gran inconveniente cuando se utiliza un miembro de la familia Catalyst 6xxx, como el MLS-SE, dado que los mismos puertos del switch pueden reconocer información de capa cuatro.

Nota: Hasta hace poco, MLS no admitía máscaras de flujo configuradas de entrada en una interfaz MLS-RP, solo de salida. Si **utiliza el comando mls rp ip input-**aclademás de los comandos de configuración MLS-RP normales en una interfaz de router, se soporta una máscara de flujo entrante.

¿Se ven más de un par de mensajes de error *MLSToo muchos* movimientos continuamente en el switch?

Como la nota menciona, para cambiar una máscara de flujo, borrar la memoria caché de ruta o desactivar globalmente el routing IP causa una purga de la memoria caché. Otras circunstancias también pueden causar purgas completas o muchas de una sola entrada y hacer que MLS se queje *de demasiados movimientos*. Existen muchas formas de este mensaje, pero cada una contiene estas tres palabras: Aparte de lo que ya se ha mencionado, la causa más común de este error es cuando el switch detecta varias direcciones MAC (del inglés Ethernet Media Access Control, control de acceso a medios) idénticas dentro de la misma VLAN; los estándares de Ethernet no permiten direcciones MAC idénticas dentro de la misma VLAN. Si se observa con poca frecuencia, o sólo unas pocas veces seguidas, no hay motivo para preocuparse; MLS es una función sólida y el mensaje puede deberse simplemente a eventos de red normales, como una conexión de PC que se mueve entre puertos, por ejemplo. Si se ve continuamente durante varios minutos, es probable que sea un síntoma de un problema más grave.

Cuando se produce esta situación, la causa raíz se debe comúnmente a la presencia de dos dispositivos con la misma dirección MAC conectada a la VLAN o a un bucle físico dentro de la VLAN (o varias VLAN si hay puentes entre estos dominios de difusión). Solucione problemas con el árbol de expansión (cubierto en otros documentos) y la sugerencia para encontrar el loop y eliminarlo. Además, cualquier cambio rápido en la topología puede provocar inestabilidad temporal de la red (y MLS) (interfaces de router inestables, una tarjeta de interfaz de red (NIC) defectuosa, etc.).

Sugerencia: Utilice los comandos **show mls notificationand show looktablecen el switch para indicarle la dirección de la dirección MAC duplicada o del loop físico.** El primero brinda un valor TA. El comando **show looktable <valor TA>** devuelve una posible dirección MAC que se puede rastrear hasta la raíz del problema.

Información Relacionada

Contenido

- Asistencia técnica y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).